This is a digital copy of a book that was preserved for generations on library shelves before it was carefully scanned by Google as part of a project to make the world's books discoverable online.

It has survived long enough for the copyright to expire and the book to enter the public domain. A public domain book is one that was never subject to copyright or whose legal copyright term has expired. Whether a book is in the public domain may vary country to country. Public domain books are our gateways to the past, representing a wealth of history, culture and knowledge that's often difficult to discover.

Marks, notations and other marginalia present in the original volume will appear in this file - a reminder of this book's long journey from the publisher to a library and finally to you.

Usage guidelines

Google is proud to partner with libraries to digitize public domain materials and make them widely accessible. Public domain books belong to the public and we are merely their custodians. Nevertheless, this work is expensive, so in order to keep providing this resource, we have taken steps to prevent abuse by commercial parties, including placing technical restrictions on automated querying.

We also ask that you:

+ *Make non-commercial use of the files* We designed Google Book Search for use by individuals, and we request that you use these files for personal, non-commercial purposes.

+ *Refrain from automated querying* Do not send automated queries of any sort to Google's system: If you are conducting research on machine translation, optical character recognition or other areas where access to a large amount of text is helpful, please contact us. We encourage the use of public domain materials for these purposes and may be able to help.

+ *Maintain attribution* The Google "watermark" you see on each file is essential for informing people about this project and helping them find additional materials through Google Book Search. Please do not remove it.

+ *Keep it legal* Whatever your use, remember that you are responsible for ensuring that what you are doing is legal. Do not assume that just because we believe a book is in the public domain for users in the United States, that the work is also in the public domain for users in other countries. Whether a book is still in copyright varies from country to country, and we can't offer guidance on whether any specific use of any specific book is allowed. Please do not assume that a book's appearance in Google Book Search means it can be used in any manner anywhere in the world. Copyright infringement liability can be quite severe.

About Google Book Search

Google's mission is to organize the world's information and to make it universally accessible and useful. Google Book Search helps readers discover the world's books while helping authors and publishers reach new audiences. You can search through the full text of this book on the web at `http://books.google.com/`

CR TX
3 2044 103 229 266

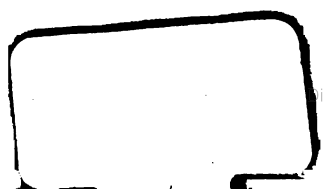
SCHNEICKERT

MODERNE GEHEIMSCHRIFTEN

GER
986.4
SCHNE

HARVARD
LAW
LIBRARY

Digitized by Google



Digitized by Google

Moderne

Geheimschriften.

Gemeinverständliche Darstellung

der

[illegible]

[illegible]

Graphologie

[illegible]

[illegible]

[illegible]

HANS SCHNEICKERT

[illegible]

[illegible]

[illegible]

Digitized by Google

Digitized by Google

Moderne

Geheimschriften.

Gemeinverständliche Darstellung

der

[illegible]

[illegible]

Graphologie

[illegible]

[illegible]

[illegible]

HANS SCHNEICKERT.

[illegible]

[illegible]

Digitized by Google

Digitized by Google

Moderne
Geheimschriften.

Gemeinverständliche Darstellung
der
gebräuchlichsten und nützlichsten Geheimschriftmethoden
mit besonderer Berücksichtigung der

Graphologie

als Hilfsmittel
zur Dechiffrierung, Verbesserung und Neubildung von Geheimschriften

von

HANS SCHNEICKERT,
Rechtspracticant,
Mitglied der „Deutschen graphologischen Gesellschaft".

Preis Mk. 3.—.

Mannheim.
Druck und Verlag der Dr. Haas'schen Druckerei.
1900.
Germany

Digitized by Google

C+W
S3584m

Nachdruck verboten.
Alle Rechte, insbesondere das der Uebersetzung, vorbehalten.

NOV 23 '26

Digitized by Google

Herrn

Dr. C. Keller, prakt. Arzt und Frau

in Rheingönheim

freundschaftlichst gewidmet.

Digitized by Google

Digitized by Google

Vorwort.

Die Geheimschreibekunst (Kryptographie, Chiffrierkunst) ist für die Diplomatie und viele staatliche Behörden in manchen Fällen ein unentbehrliches Mittel der Verständigung und wird in ihren Ressorts schon sehr lange gepflegt und verbessert. Im Laufe der Zeit fanden aber auch andere Kreise nicht nur ein Verständnis für die Geheimschreibekunst, sondern die Lage der verschiedensten Verhältnisse brachte auch den Bankier, den Kaufmann, selbst den Gefangenen und Verbrecher dazu, eine bereits bekannte Geheimschriftmethode zur geheimen Verständigung seines Genossen zu verwenden, oder — was zuweilen der Fall ist — eine neue Methode zu construieren. — So sind in neuerer Zeit die alten, mitunter ganz wertvollen Geheimschriftmethoden namentlich durch den Scharfsinn von Verbrechern in unglaublich raffinierter Weise übertroffen worden.

Ich machte es mir nun zur Aufgabe, neben der Darstellung der älteren, heute noch vielfach benutzten Geheimschriftmethoden durch Einsicht in die ziemlich umfangreiche Litteratur der Kryptographie eine Zusammenstellung der bewährtesten Methoden zu geben, die dem Laien einerseits einen Einblick gewähren in das interessante Gebiet der Chiffrierkunst, andrerseits bei der Wahl und Anwendung einer Geheimschriftmethode die nötigen Winke geben soll. — Daher richtete ich auch ein besonderes Augenmerk auf eine leicht fassliche und durch Beispiele illustrierte Erklärung der einzelnen Methoden, wies auf die Mängel der einzelnen Methoden — soweit solche bestehen — hin und versuchte, jeweils Mittel und Wege zu finden, dieselben zu mindern oder zu beseitigen. So wird auch die Möglichkeit geboten, durch beispielsweise Anwendung von vielen erdenklichen Variationen nach eignem Bedarf und Geschmack eine Methode für sich verwendbar zu machen, sodass sich immerhin ein individueller Wert dieses Werkchens ergeben mag.

Im dritten Abschnitt dieser Darstellung unternahm ich es, die Kryptographie von einem bis jetzt wohl noch nicht berück-

Digitized by Google

sichtigten, nämlich vom graphologischen Standpunkt aus zu betrachten, indem ich durch feststehende Grundsätze der Graphologie einen Wert derselben für die Entzifferung, Verbesserung, sowie Neubildung von Geheimschriften nachzuweisen versuchte.

Schliesslich sei an dieser Stelle noch die einschlägige — bis jetzt publizierte — Litteratur, die zu eingehenden Studien hinreichend Material bietet, verzeichnet:

J. H. Schooling: The pall mall magazine, London, W. C. vol. VIII. No. 33—36. 1896.
E. B. Fleissner: Handbuch der Kryptographie. Wien 1881.
A. Walter: Chiffrier- und Telegraphiersystem, Winterthur 1877.
C. Krohn: Buchstaben- und Zahlensysteme für die Chiffrierung von Telegrammen, Briefen und Postkarten, Berlin 1873.
F. W. Kasiski: Die Geheimschriften und die Dechiffrierkunst, Berlin 1863.
C. L. Meissner: Die Correspondenz in Chiffern, Braunschweig 1849.
Klüber: Kryptographik, Tübingen 1809.

Ludwigshafen a. Rh., im August 1900.

Der Verfasser.

Digitized by Google

Inhalt.

Seite

Einleitung 1

Erster Abschnitt.

Geheimschriften mit Hilfe der Buchstaben und Ziffern. 2—54

Allgemeine Regeln über die Anwendung einer Geheimschriftmethode 2—4

Buchstabenchiffriermethoden.

I. Methode Caesars . . . . . 4—6
II. Die hebräische Methode . . . . . 6—7
III. Die chinesische Methode und die Methode im Zickzack oder in der Schlangenlinie . . . . . 7—8
IV. Methode in der Diagonale . . . . . 8—10
V. Methode im Parallelogramm . . . . . 10—11
VI. Tritheims Multiplikationschiffre (1—3) . . . . . 11—15
4. Chiffreschrift des Grafen Gronfeld . . . . . 15—16
VII. Chiffriermethode Napoleons I. . . . . 16—18
VIII. Methode durch Bildung neuer Wörter . . . . . 19—21
IX. Methode Richelieu's . . . . . 21—22
X. Der Netz- oder Gitterchiffre . . . . . 22—27
XI. Fleissners neue Patronengeheimschrift . . . . . 27—31
XII. 1. Der Circularscheibenchiffre . . . . . 31—32
2. Der Leiterchiffre . . . . . 32—34
XIII. Bacon's Vermehrungschiffre . . . . . 34—36
XIV. Der Wort- und Silbenchiffre 36
XV. Der Vokalchiffre . . . . . 36—37
XVI. a) Geheimschrift eines Nihilisten. . . . . 37—39
XVII. b) „ „ „ . . . . . 39—40
XVIII. c) „ „ „ . . . . . 41—42
XIX. Chiffriermethode mit Anwendung mehrerer Alphabete . . . . 42—44

Zahlenchiffriermethoden.

XX. Kircher's abacus numeralis 45
XXI. Ein Zahlenchiffre nach Caesar's Methode 45
XXII. Mirabeau's Methode . . . . . 45—46
XXIII. Ein Zahlenchiffre mit wechselndem Alphabet 47
XXIV. Ein Zahlenchiffre mit Rechenoperationen . . . . . 48—49
XXV. Der Massstabchiffre . . . . . 49—50

Punktiermethoden.

XXVI. Schotti's Punktiermethode . . . . . 51—52
XXVII. Heidel's „ „ . . . . . 52—53
XXVIII. Der Buchchiffre . . . . . 53—54

Digitized by Google

Zweiter Abschnitt.

Geheimschriften mit Hilfe anderer Zeichen.

Seite

I. Gemischte Chiffriermethode . . . . . 56—57
II. Der Winkel- und Quadratchiffre (Maurerchiffre) . . . . . 57—58
III. Der Musik- oder Notenchiffre . . . . . 58—59
IV. Chiffriermethoden unter Anwendung von geraden u. gebogenen Linien. — Punktiermethoden . . . . . 59—64
1. Der Linienchiffre 60
2. Einige Punktiermethoden . . . . . 60—62
3. Der Massstabchiffre . . . . . 62—63
4. Der Fadenchiffre . . . . . 63—64
V. Der Kartenchiffre 64
Methode der Lacedaemonier 64
VI. Sympathetische Tinten 65

Dritter Abschnitt.

Kryptographie und Graphologie.

a. Die Graphologie als Hilfsmittel zur Dechiffrierung von Geheimschriften . . . . . 68—82
I. Fleissner's neue Patronengeheimschrift . . . . . 68—70
II. Der Netz- oder Gitterchiffre . . . . . 71—73
III. Boetzel's Methode . . . . . 73—77
IV. Geheimschrift eines Nihilisten . . . . . 77—82
b. Die Graphologie als Hilfsmittel zur Bildung neuer Geheimschriften . . . . . 82—87
V. Graphologische Geheimschriftmethoden . . . . 82—87
1. Die stenographologische Punktiermethode . . . . . 82—85
2. Die Schrifteigenheits-Punktiermethode . . . . . 85—86

Anhang.

Drei neue Geheimschriftmethoden.

1. Der Orthographiechiffre . . . . . 88—89
2. Der Referatchiffre . . . . . 89—90
3. Die Reduktionsmethode . . . . . 91—92
Schlusswort 93

Digitized by Google

Einleitung.

„Briefe sind unsere schlimmsten Feinde", sagt ein bekanntes Sprichwort. Die Wahrheit dieses Satzes wird mancher schon selbst erfahren haben. — Gegen die unbefugte Eröffnung eines Briefes von seiten der Post sind allerdings gesetzliche Vorkehrungen getroffen durch § 354 des Strafgesetzbuches für das deutsche Reich; aber auch die vorsätzliche und unbefugte Eröffnung eines Briefes von seiten jedes Dritten ist durch den § 299 des cit. Strafgesetzbuches mit Strafe bedroht. — In dieser Hinsicht ist also das Briefgeheimnis schon geschützt, und soweit dieser Schutz reicht, wird auch der oben genannte Satz nicht zur eigentlichen Geltung kommen. Anders aber nach der Eröffnung des Briefes durch den Berechtigten. Durch Zufall oder durch Unvorsichtigkeit des Besitzers eines Briefes kann dieser in unberechtigte Hände gelangen und oft grosse Unannehmlichkeiten verursachen. Zur Vermeidung eines solchen Falles wird man bestrebt sein, Vorsichtsmassregeln zu treffen, um die Gefahr der unbefugten Kenntnisnahme einer höchst privaten Mitteilung zu beseitigen: man greift zum einzig sicherstellenden Hilfsmittel — zur „Geheimschrift", wobei man sich einer bekannten Geheimschriftmethode bedient, oder mit seinem Correspondenten eine „eigene" Verständigungsweise in Gestalt einer variierten Chiffriermethode vereinbart. — So wird auch die Briefform überflüssig, und man erreicht auf billigerem Wege schon durch eine Postkarte dasselbe Ziel. Zugleich erleichtert man dadurch dem Post- und Telegraphenbeamten die Wahrung des Briefgeheimnisses.

Digitized by Google

Erster Abschnitt.

Geheimschriftmethoden mit Hilfe der Buchstaben und Ziffern.

Allgemeine Regeln über die Anwendung einer Geheimschriftmethode.

Ehe ich die einzelnen Geheimschriftmethoden selbst näher bespreche, will ich zuerst einige fundamentale Regeln zur besseren Sicherung des Geheimnisses vorausschicken und bei Anwendung einer Geheimschriftmethode zur Beachtung empfehlen.

Welcher Art die „Geheimschrift" auch sei — ob ein Gebilde aus Buchstaben, Ziffern, Satzzeichen oder anderen vereinbarten Zeichen — stets hüte man sich vor auffälliger Bezeichnung vom Absendungsorte und Datum in Chiffreschrift (was ja zumeist aus dem Poststempel ersichtlich wäre), ferner von Anreden und Schlusswendungen, die dem unbefugten Dechiffreur leicht auf eine Spur verhelfen könnten. Weiter vermeide man, Wörter oder Sätze im Zusammenhang der geheimen Mitteilung in Klarschrift (en clair) zu schreiben. — Im allgemeinen verzichte man auch (wie bei den Stenographiesystemen) auf Verdoppelungen (Verschärfungen und Dehnungen) sowie auf Interpunktions- und Trennungszeichen, sofern dadurch nicht der Sinn der Mitteilung verändert würde.

Grosse Buchstaben (Majuskeln) sind überall zu vermeiden, namentlich wenn sie denen der Klarschrift entsprächen.

Ein Vorteil ist es auch, die einzelnen Chiffrezeichen womöglich verbunden aneinanderzureihen, oder beliebig grosse (am besten jeweils gleich grosse) Gruppen von Wörtern zu bilden, (um die Anzahl der Buchstaben eines Wortes der Klarschrift nicht erkennbar zu machen), natürlich wenn dies nicht die Methode an und für sich verhindert; im letzteren Falle können eingeschaltete nichts bedeutende Buchstaben oder Zeichen*) die notwendige

*) sog. non-valeurs oder Nieten.

Digitized by Google

Trennung zwischen zwei Wörtern verschmelzen. Das Einschalten von nichts bedeutenden, irreführenden Zeichen oder Buchstaben ist überhaupt überall zur Anwendung zu empfehlen. — Von den 29 Buchstaben des Alphabetes, wobei *ä, ö, ü* und *j* noch eingeschlossen werden, kann man mindestens 8 Buchstaben entbehren und als Nieten benutzen; dabei setzt man für *c=k* oder *z*, für *j=i*, für *q=kw*, für *x=ks*, für *y=i*.

Ausserdem kann man, soweit man nicht irgend eine besondere Versetzungsmethode anwenden will, die bereits chiffrierte Mitteilung dadurch verwirren, dass man die einzelnen Wörter oder deren Silben von rückwärts schreibt, z. B. Art—tra, Blu | me—ulbem.

Für die Umlaute *ä, ö, ü* setzt man im allgemeinen am besten *ae, oe, ue* oder (wie bei der Stenographie) *e, e, i;* für die Ziffern kann man besondere Zeichen vereinbaren oder sie, der Aussprache entsprechend, als Wörter behandeln, z. B. 3 = drei.

Es ist auch ganz entschieden vorteilhaft, zeitweise die anzuwendende Methode zu variieren oder zu wechseln, was durch besonders verabredete Zeichen (Changierzeichen) anzudeuten ist; so werden etwa entdeckte Spuren der Entzifferung von seiten eines Dritten wieder zu nichte gemacht.

Als irreführende Zeichen können auch sog. Anullierungs- und Gegenteils- (oder Widersinns-) -zeichen in die Chiffreschrift eingeführt werden, die das Vorhandensein gewisser Wörter oder Sätze vernichten resp. deren Gegenteil constatieren sollen: z. B. eine anullierte Negation, oder die Anwendung des Wortes Freund statt Feind etc. sollen mit jenen Zeichen dem Correspondenten erkennbar gemacht werden.

Es gibt manche Chiffriermethoden, die erst dadurch, dass sie mit einer anderen verbunden werden, genügend zuverlässig werden. Deshalb hielt ich es für angemessen, im Anfange dieses Abschnittes den Leser mit den geeignetsten Versetzungsmethoden (Methoden I—V, VIII, IX, X, XI) bekannt zu machen und ihm dieselben zur Auswahl zu stellen.

Schliesslich will ich hier noch bemerken, dass im telegraphischen Verkehr die Chiffreschrift, soweit sie nur aus Buchstaben, arabischen Ziffern und Satzzeichen (in ihrer naturgemässen Anwendung) besteht, zulässig ist.*)

---

*) Dies gilt jetzt nicht mehr für Privattelegramme. Sh. unten.

Digitized by Google

Die internationalen Bestimmungen für den geheimen telegraphischen Verkehr, die hier in Betracht kommen, sind kurz folgende:

Der Text eines Telegrammes kann entweder ganz oder nur teilweise geheim sein; in letzterem Falle müssen die geheimen Stellen durch Klammern von dem übrigen Text ausgeschieden werden. Die in Ziffern- oder Buchstabengruppen geschriebene Geheimschrift wird nach je 5 Ziffern oder Buchstaben abgeteilt und als einzelne Wörter behandelt, wobei ein etwaiger Ueberrest von Ziffern oder Buchstaben als ein ganzes Wort betrachtet wird. — Einzelstehende Schriftzeichen werden je für ein Wort gezählt, ebenso Unterstreichungszeichen; Interpunktionen, Bindestriche, Apostrophe, Anführungszeichen und Klammern werden nicht gezählt; aber Punkte, Beistriche und Bruchstriche, die zur Bildung der Zahlen gebraucht werden, werden für je eine Ziffer gezählt.

Kürzlich gab die Post eigene Telegraphiewörterbücher heraus, in denen die Wörter verzeichnet sind, welche ausschliesslich zur Benützung bei chiffrierten Privattelegrammen zugelassen werden.

I.

Methode Caesars.

Eine sehr einfache und kunstlose Methode der Geheimschrift (Versetzungsmethode), die darum auch (in ursprünglicher oder variierter Gestalt) meistens die Eingangspforte in die Kryptographik für den Correspondierenden bildet, stellt die Geheimschriftmethode Julius Caesars dar. Sie besteht darin, dass die einzelnen Buchstaben des Alphabetes gegenseitig vertauscht werden.

Der Schlüssel zu diesem Versetzungs-Chiffre wäre z. B.:

a b c d e f g h i k l m n o p q r s t u v w x y z
f d g e o w u b n x q a v t c m l p h s y i z r k

Hiernach hiesse die Mitteilung:

Ich erwarte Antwort:
ngb oiflho fvhitlh.

Die Methode hat nun zunächst den offensichtlichen Mangel, dass ein Buchstabe jedesmal durch einen anderen, aber stets gleichen Buchstaben bezeichnet werden muss; z. B. zeigen die beiden *l* im Worte oiflho an, dass zweimal der gleiche Buchstabe

Digitized by Google

hier auftritt. Ein einigermassen geübter Dechiffreur weiss aber, dass in der deutschen Sprache an erster Stelle der Buchstabe *e* am häufigsten auftritt, an zweiter Stelle der Buchstabe *n*, an dritter Stelle *i*, an vierter Stelle *r* etc. Wenn dann in einem nach dieser Methode chiffrierten Schriftstücke ein Buchstabe vor allen anderen sehr häufig auftritt, so wird dies mit Sicherheit darauf schliessen lassen, dass es der Vocal *e* ist. In dieser Hinsicht sind also leicht Spuren zur Entzifferung zu entdecken.

Ein weiterer Mangel ist die der Klarschrift entsprechende Anzahl der Buchstaben eines Wortes. Die Anzahl der zwei- und dreisilbigen Wörter (d. i. der Bigramme und Trigramme) in der deutschen Sprache ist ziemlich beschränkt, sodass es oft nicht schwierig wäre, ein solches an bestimmter Stelle zu erraten.

Man weiss aber diese Mängel einigermassen zu umgehen, indem man verschiedene Kunstgriffe anwendet. So schreibt man z. B. die chiffrierte Mitteilung ohne jegliche Trennung zwischen den einzelnen Wörtern, oder man nimmt beliebige Trennungen der Wörter vor, oder man schiebt sog. Nieten (nichtsbedeutende Schriftzeichen) ein, wobei auch griechische, russische, hebräische etc. Buchstaben verwendet werden können. Der beste Kunstgriff ist aber der, die bereits chiffrierte Mitteilung nach einer anderen bekannten Methode nochmals zu chiffrieren.

Der Empfänger der chiffrierten Mitteilung wird absolut keine Schwierigkeit haben, dieselbe zu entziffern, indem er seinen Schlüssel hernimmt und nach Entfernung der Nieten die Versetzung der einzelnen Buchstaben in umgekehrter Weise (wie oben) bewerkstelligt.

Die Art der Auffindung eines neuen Alphabetes in diesem Genre unterliegt der freien Phantasie jedes einzelnen und ist höchst mannigfaltig.

Eine Variation dieser Methode ist die Ersetzung der einzelnen Buchstaben durch Zahlen.*) Es soll z. B. $a=8$, $b=5$, $c=9$, $e=14$ etc. bedeuten. Auch hier werden ähnliche Kunstgriffe erforderlich sein, um die auftretenden Mängel zu beseitigen.

Diese einfache Methode bietet für den sie Gebrauchenden überhaupt keine Schwierigkeit im Erlernen und bei ihrer Anwendung; sehr schnell hat sich das verabredete Alphabet dem Gedächtnisse eingeprägt, sodass ein schriftlicher Schlüssel bald entbehrlich wird.

---

*) Vgl. hierzu Methode XXI dieses Abschnittes.

Digitized by Google

Krohn hat auf diese Weise 3200 verschiedene Alphabete in seinem Werke zusammenzustellen sich die Mühe gegeben, die aber im Princip an den gleichen Mängeln wie Caesars Methode leiden.

II.

Die hebräische Methode.

Eine weitere Methode, die sich dazu eignet, bereits chiffrierte Depeschen zu verwirren, ist die sog. hebräische Methode. Dieselbe ermöglicht gemäss der eigenartigen Schreibweise der hebräischen Schrift eine Versetzung der Buchstaben der geheimen Mitteilung in der Richtung, dass von rechts nach links geschrieben wird. Die Mitteilung:

Wie verabredet, besuche ich Dich

nähme folgende Gestalt an nach dem Chema:

11 10 9 8 7 6 5 4 3 2 ← 1
etc. 15 14 13 12

r	b	a	r	e	v	e	i	w
c	u	s	e	b	t	e	d	e
h	c	i	d	h	c	i	e	h

Also: rbareveiwcuse etc.*)

1. Variation: Chema: etc. 14 13 12 11 10 9
8 7 6 5 4 3 2 ← 1

								h	c	i	
d	h	c	i	e	h	c	u	s	e	b	t
e	d	e	r	b	a	r	e	v	e	i	w

Also: hcidhciehcus etc.

2. Variation: Chema: 9 8 7 6 5 4 3 ← 2 1
→ 10 11 12 13 14 15 16 17 18
etc. 21 20 19
→ etc. 16 15

3. Variation: Chema: 8 9 10 11 12 13 14
7 6 5 4 3 2 ← 1

Die beiden letzten Variationen führen auch den Namen „Methode im Zickzack“ oder „in Schlangenlinie“ mit Rücksicht auf die Art der Fortbewegung in der Reihenfolge. (Vgl. unten Methode III, Variation 6 und 7.)

*) Die chiffrierte Mitteilung kann auch z. B. lauten: rchbucasir etc. oder hcrbucisar etc., je nachdem man verabredungsgemäss die Chiffrebuchstaben ablesen will. Also schon beim Ablesen der Chiffrebuchstaben lässt sich eine weitere Versetzungsmethode (Methode II und folg. dieses Abschnittes) anwenden; so auch bei den nachfolgenden Beispielen.

Digitized by Google

4. Variation: Es soll jedesmal der übernächste (oder der 3. oder der 4. nächste) Buchstabe Geltung haben, während die übrigen dazwischenliegenden nur als irreführende Nieten zu behandeln sind.

Z. B.

×		×		×		×		×		×		×
a	v	r	n	e	d	v	k	e	l	i	f	w
l	t	z	e	u	d	r	e	i	r	c	b	l
etc.		h	o	c	b	u	x	s	k	e	p	b

Also: avrnedvkelifwlt etc.***)

Diese (4.) Variation lässt sich auch leicht mit der 1., 2. und 3. Variation verbinden.

Der Empfänger der chiffrierten Mitteilung wird bei Kenntnis des Verfahrens bei der verabredeten Variation ohne jede Schwierigkeit die Chiffreschrift dechiffrieren können, wenn er die Buchstaben der übersandten Mitteilung (wie oben) in die einzelnen Felder des Rechteckes in gegebener Reihenfolge einträgt.*)

III.

Die chinesische Methode und die Methode im Zickzack oder in der Schlangenlinie.

Nun kann man aber die Buchstaben anstatt nebeneinander- auch untereinanderschreiben, wie dies die chinesische Schreibart erfordert; daher auch chinesische Methode genannt.

Obige Mitteilung nimmt nach dem Chema:**)

	13	9	5	1 ↓
	14	10	6	2
	etc.	11	7	3
		12	8	4

folgende Gestalt an:

	i	s	d	r	w
	c	u	e	a	i
	h	c	t	b	e
	etc.	h	b	r	v
		e	e	e	e

Also: isdrwcueaihc etc.***)

1. Variation: Chema:

		12	8	4
	etc.	11	7	3
	14	10	6	2
	13	9	5	1 ↑

*) Vgl. hierzu III. Abschnitt. I. Cap. dieser Darstellung.

**) Das Einsetzen der Buchstaben in diesem wie in allen folgenden Chematen hat stets nach der natürlichen Reihenfolge der Zahlen (1, 2, 3, 4, 5, 6, 7 etc.) zu geschehen.

***) Sh. auch die Fussnote auf S. 6.

Digitized by Google

2. Variation: Chema:

↓ 1	5	9	13					
2	6	10	14					
3	7	11	etc.					
4	8	12						

3. Variation: Chema:

4	8	12		
3	7	11	etc.	
2	6	10	14	
↑ 1	5	9	13	

4. Variation: Chema:

↓ 1	8	9			
2	7	10	etc.		
3	6	11	14		
4	5	12	13		

↑ ↓

5. Variation: Chema:

4	5	12	13		
3	6	11	14		
2	7	10	etc.		
↑ 1	8	9			

6. und 7. Variation: Anfang rechts oben bezw. rechts unten, wobei jeweils die einzelnen Colonnen im Zickzack oder in Schlangenlinie (d. h. in verbundener Reihenfolge wie bei Variation 4 und 5) mit den Chiffrezeichen ausgefüllt werden. Daher haben auch die vier letzten Variationen die Bezeichnung: Methode im Zickzack oder in der Schlangenlinie.*)

Ueber das Einschieben von Nieten und über die Dechiffrierung gilt das oben (bei Methode I und II) Gesagte.

IV.

Methode in der Diagonale.

Die Buchstaben können ferner in der Diagonale aufeinanderfolgen: Methode in der Diagonale.

*) Vgl. hierzu III. Abschnitt, I. Cap. dieser Darstellung; ferner Methode II, Variation 2 u. 3 dieses Abschnittes.

Digitized by Google

Obige Mitteilung erhält hiernach folgende Gestalt:

Chema:

1	3	6	10	
2	5	9		
4	8		etc.	
7				

w	e	r	e	
i	e	r		
v	b	t	etc.	
a	e			
d				

Also: wereiervbt etc.*)

1. Variation: Chema:

1	2	4	7	11	
3	5	8	12		
6	9	13			
10	14				
15	etc.				

2. Variation: Chema:

1	3	4	10	11	
2	5	9	12		
6	8	13	16	etc.	
7	14	15			

3. Variation: Chema:

1	2	6	7	
3	5	8		
4	9	12	etc.	
10	11			

4. Variation: Chema:

				5				
			4	13	6			
		3	12	19	14	7		
	2	11	18	23	20	15	8	
1	10	17	22	25	24	21	16	9

*) Sh. auch die Fussnote auf S. 6.

Digitized by Google

Weitere Variationen*) ergeben sich, wenn man an einer anderen Stelle der Chemata nach der angegebenen Weise beginnt, oder sonstwie die Reihenfolge ändert; z. B.

				5				
			4	13	6			
		3	14	19	12	7		
	2	15	18	23	20	11	8	
1	16	17	24	25	22	21	10	9

Hiernach müsste die oben angegebene Mitteilung chiffriert werden, wie folgt:

				e				
			v	t	r			
		e	b	h	e	a		
	i	e	c	h	e	d	b	
w	s	u	d	i	c	i	e	r

Also: evtrebheaieched etc.**)

Ueber Nieten und Dechiffrierung vergl. Methode I und II.***)

V.

Methode im Parallelogramm.

Endlich lassen sich die Buchstaben einer Mitteilung nach der Methode im Parallelogramm versetzen.

Chema:

1 2 3 4 5 6 7 8 18
19 20 21 22 36
37 38 39 40 54
55 56 etc.

*) Vgl. hierzu III. Abschnitt, I. Cap. dieser Darstellung.
**) Sh. auch die Fussnote auf S. 6.
***) Vgl. auch die zweite Fussnote auf S. 7.

Digitized by Google

Die Reihenfolge der Buchstaben der zu chiffrierenden Mitteilung ist:

1; 19, 2; 37, 20, 3; 55, 38, 21, 4 etc., weil 19 und 2
37, 20 und 3 etc.
auf einer Diagonale von links unten nach rechts oben liegen,

Chema hierzu:

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	·	·	·

z.B.

w	i	e	v	e	r	a	b	r	e
d	e	t	b	e	s	u	c	h	e
i	c	h	d	i	c	h	·	·	·

Also: wdiieectvhbe etc.*)

Indem man dieses Chema in entsprechender Weise wie in den vorhergehenden Methoden behandelt, erhält man wieder mehrere Variationen.

Beim Dechiffrieren der obigen geheimen Mitteilung müssen deren einzelne Buchstaben in der Diagonale nach dem Chema:

1	3	6	9	12			
2	5	8	11	14	etc		
4	7	10	13				

aufgezeichnet werden.**)

VI.

Tritheims Multiplikationschiffre.

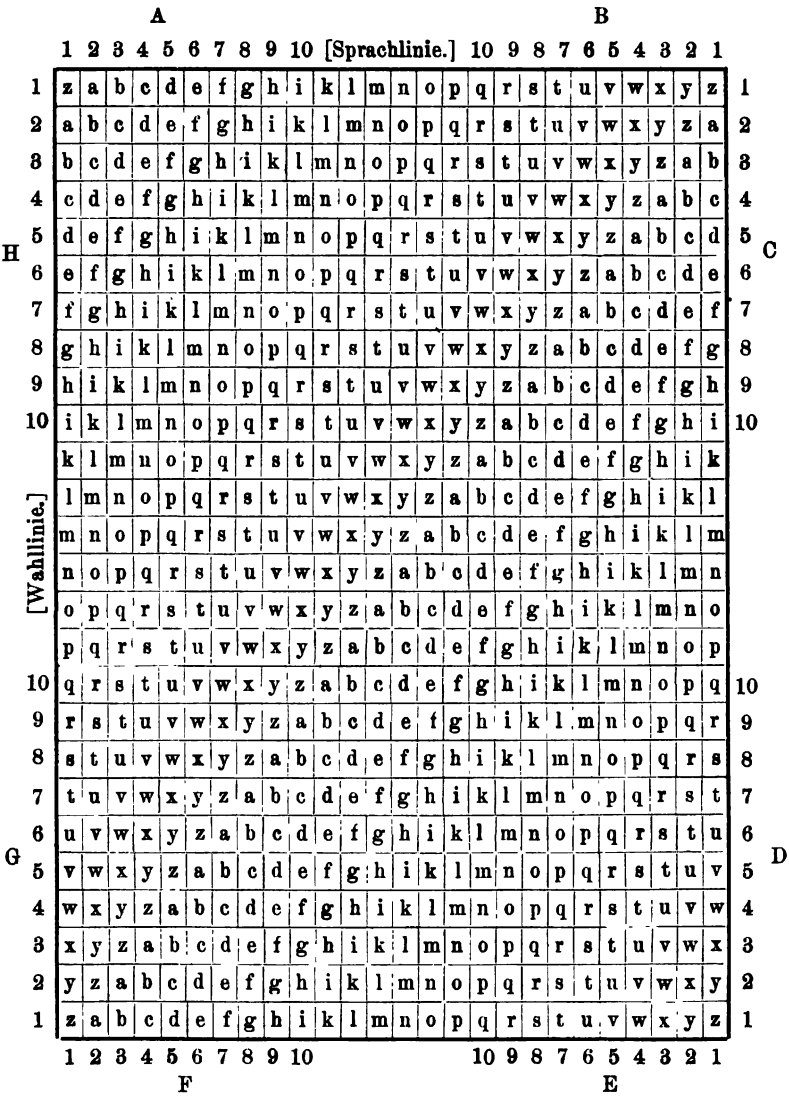
Ein altes Verfahren, das aber heute noch vielfach im Gebrauch ist, ist der sogenannte chiffre carré oder indéchiffrable (Multiplikationschiffre); die eigentliche Entstehung dieses Systems wird auf den Benediktiner Tritheim (Trithemius 1462—1516) zurückgeführt. Der Schlüssel dieses Systems besteht aus einer Tabelle, dessen Quadrate durch die 25 Buchstaben des Alphabetes in folgender Weise ausgefüllt werden.***)

*) Sh. auch die Fussnote auf S. 6.

**) Vgl. hierzu III. Abschnitt, I. Cap. dieser Darstellung. Ferner Methode IV dieses Abschnittes.

***) Bezüglich der Bezeichnungen auf dem Rand der Tabelle vgl. die Anmerkung zur Gronfeld'schen Chiffreschrift. (S. 15.)

Digitized by Google



1. Die erste Horizontalreihe heisst hier die „Sprachlinie“, die erste Vertikalreihe links heisst „Wahllinie“. Der Schlüssel des Geheimnisses bildet ein beliebig gewähltes Wort (Wahlwort), dessen einzelne Buchstaben in natürlicher Reihenfolge unter die einzelnen Buchstaben der zu chiffrierenden Mitteilung gesetzt werden, wobei man das Unterschreiben mit dem stets wiederholten Wahlwort fortsetzt bis zum letzten Buchstaben der geheimen Mitteilung.

Digitized by Google

Das Wahlwort sei z. B. Traum, die geheime Mitteilung: „Erwarte mich“,

also: e r w a r t e m i c h
t r a u m t r a u m t

Den Chiffrebuchstaben findet man nun, indem man den daruntergeschriebenen Buchstaben des Wahlwortes (t . . .) in der Wahllinie und den entsprechenden Buchstaben der Mitteilung (e . . .) in derselben Horizontalreihe, welcher jener angehört, aufsucht. Indem man sodann die Vertikalreihe des Buchstabens der geheimen Mitteilung bis zur Sprachlinie verfolgt, findet man den Chiffrebuchstaben (l . . .).

l z v f e z n l o q o
Also: { e r w a r t e m i c h }
{ t r a u m t r a u m t }

Um nun die geheime Mitteilung: lzvfeznloqo zu entziffern, schreibt man wieder — wie oben — das Wahlwort darunter:

l z v f e z n l o q o
t r a u m t r a u m t

Jetzt wird *t* (r, a etc.) in der Wahllinie wieder aufgesucht und *l* (z, v etc.) in der Sprachlinie; wo nun die Horizontalreihe von *t* (r, a etc.) auf die Vertikalreihe von *l* (z, v etc.) trifft, also bei *e* (r, w etc.), da steht der Buchstabe der entzifferten Mitteilung.

Diese Tabelle lässt aber ausserdem noch eine Reihe Variationen zu. Dasselbe Resultat wie oben erhält man, wenn man in entsprechender Weise von der Sprachlinie (statt der Wahllinie) ausgeht. Der zu suchende Chiffrebuchstabe wird hierbei in der Wahllinie (statt in der Sprachlinie) stehen.

2. Ein anderes Resultat erhält man, wenn man zuerst den Buchstaben der zu chiffrierenden Mitteilung in der Wahllinie (bezw. Sprachlinie) und dann den unter ihm stehenden Buchstaben des Wahlwortes in derselben Horizontalreihe (bezw. Vertikalreihe), welcher jener angehört, aufsucht. Wenn man hierauf die Vertikalreihe (bezw. Horizontalreihe) des Buchstabens des Wahlwortes bis zur Sprachlinie (bezw. Wahllinie) verfolgt, findet man den Chiffrebuchstaben.

Also: { e r w a r t e m i c h }
{ t r a u m t r a u m t }
o z d t u z m o l i l

Die geheime Mitteilung: ozdtuzmolil wird genau in der oben (unter 1) angegebenen Weise dechiffriert.

Digitized by Google

3. Weiterhin lässt sich mit Hilfe der obigen Tabelle ein neues geheimes Alphabet construieren, indem man jeden Buchstaben der zu chiffrierenden Mitteilung als Kreuzpunkt je einer Horizontal- und Vertikalreihe ansieht. Eines Wahlwortes bedarf es hier also nicht. Auf diese Weise wird ein Buchstabe der Mitteilung jedesmal durch zwei Buchstaben bezeichnet, von denen der eine der äusserste Buchstabe der Horizontalreihe, der andere der äusserste Buchstabe der Vertikalreihe ist, (ohne Unterschied auf rechts und links, oben und unten).

Z. B. nr = e, d. h. die Horizontalreihe (bezw. Vertikalreihe) von *n* in der Wahllinie (bezw. Sprachlinie) trifft die Vertikalreihe (bezw. Horizontalreihe) von *r* in der Sprachlinie (bezw. Wahllinie) an der Stelle, wo der Buchstabe *e* steht. Also ist e = nr (oder auch rn), f = mt (oder tm), l = rt (oder tr) etc.

Um nun aber dem Mangel der Methode sub I abzuhelfen, wird man in dem Falle, dass der gleiche Buchstabe in demselben Wort zum zweiten oder dritten Male vorkommt, denselben nicht wie das erste Mal bezeichnen. Die Tabelle ermöglicht es, einen Buchstaben nach dieser Variation in 25-facher Weise zu bezeichnen. Z. B. t = as, br, cq, dp, eo, fn, gm, hl, ik, ki, lh, mg, nf, oe, pd, qc, rb, sa, tz, uy, vx, ww, xv, yu, zt. —

Die Sicherheit des Geheimnisses, speciell bei dieser Variation, hängt lediglich von der Geheimhaltung und vorsichtigen Benützung des Schlüssels ab. Unter solchen Umständen kann diese Art der Geheimschrift einfach undechiffrierbar werden.

Wieder ein anderes Resultat erhält man, wenn man Variation 1 und 3 in der Weise mit einander verbindet, dass der Kreuzpunkt durch die mit dem Buchstaben des Wahlwortes (t) und dem Buchstaben der Mitteilung (e) beginnende Horizontal- bezw. Vertikalreihe gebildet wird; also et = y, rr = i, wa = x, au = v, rm = d etc.

Was die eigentliche Methode (gegründet auf ein gewähltes Wort) anbelangt, so ist es ohne Kenntnis des geheimen Wahlwortes dem Uneingeweihten geradezu unmöglich, die Geheimschrift nach diesem Verfahren gebildet, zu entziffern, auch wenn er im Besitze der Tabelle wäre. Bemerkenswert ist es, dass durch diese Methode gleiche Buchstaben der Mitteilung in der Regel nie durch den gleichen Chiffrebuchstaben bezeichnet werden, was ein bedeutender Vorzug derselben ist.

Digitized by Google

Die Leichtigkeit des Gebrauches und die Möglichkeit, mit Hilfe dieser Tabelle verschiedene Geheimschriften zu bilden, ferner die gebotene Sicherheit empfiehlt diesen Multiplikationschiffre in jeder Hinsicht zur geheimen Correspondenz. —

---

4. Bei dieser Methode will ich noch Erwähnung thun der Chiffreschrift des Grafen Gronfeld, weil sie nach meiner Ansicht mit Hilfe obiger Tabelle sehr bequem anzuwenden ist.*) Statt eines Wahlwortes bedient sich Gronfeld einer gewählten Zahl (Wahlzahl), die in gleicher Weise wie das Wahlwort unter die zu chiffrierende Mitteilung gesetzt wird, sodass unter jedem Buchstaben eine Ziffer steht; der zu suchende Chiffrebuchstabe ist nun derjenige Buchstabe, welcher um soviel Stellen später in der gewöhnlichen Reihenfolge des Alphabetes erscheint, als die darunter stehende Ziffer anzeigt.

Die Wahlzahl heisst z. B. 4 8 2 1 6; die Mitteilnng: „Ich erwarte Dich“ soll nach dieser Methode chiffriert werden:

	i	c	h	e	r	w	a	r	t	e	d	i	c	h
	4	8	2	1	6	4	8	2	1	6	4	8	2	1
Also:	n	l	k	f	x	a	i	t	u	l	h	r	e	i

Am bequemsten zählt man natürlich von der Sprachlinie oder der Wahllinie aus (also von oben nach unten oder von links nach rechts).

Der zu suchende Chiffrebuchstabe kann nun auch derjenige sein, welcher um soviel Stellen früher in der gewöhnlichen Reihenfolge des Alphabetes steht, als die darunterstehende Ziffer angibt; hierbei zählt man also vom rechten Ende der Tabelle nach links, oder vom unteren Ende derselben nach oben.

	i	c	h	e	r	w	a	r	t	e	d	i	c	h
	4	8	2	1	6	4	8	2	1	6	4	8	2	1
Also:	e	u	f	d	l	s	s	p	s	y	z	a	a	g

Soll nun die geheime Mitteilung eufdlsspsyzaag dechiffriert werden, so setzt man, wie oben, die Wahlzahl unter diese Buchstaben, beginnt auf der Tabelle von der D-Seite aus bei der Ziffer nach links (Horizontalreihe) zu suchen, die um 1 grösser ist als die

---

*) Zur Anwendung dieser Methode sowie meiner hierbei angeführten Variationen versah ich obige Tabelle mit Ziffern und Buchstaben, deren Bedeutung sich aus den an dieser Stelle gegebenen Beispielen ergibt.

Digitized by Google

daruntergeschriebene Ziffer der Wahlzahl, bis man den betreffenden Buchstaben der geheimen Mitteilung auffindet; der äusserste Buchstabe in der Vertikalreihe des Chiffrebuchstabens oben oder unten stellt nun den gesuchten Buchstaben der Klarschrift dar. —

Ebenso kann man auf der Tabelle bei E beginnen, muss dann aber die Horizontalreihe des Chiffrebuchstabens bis zum linken oder rechten Ende verfolgen, um den chiffrierten Buchstaben zu finden. — Das gleiche Resultat ergibt sich, wenn man statt bei D (bezw. E) auf der entgegengesetzten Seite bei G (bezw. B) nach rechts (bezw. nach unten) den Chiffrebuchstaben zu suchen beginnt. —

Ganz ähnlich liegt die Sache im ersten Falle bei der geheimen Mitteilung: nlkfxaitulhrei. Man beginnt hier bei A (bezw. F) und verfolgt die Horizontalreihe des Chiffrebuchstabens bis zu einem Ende, wo der dechiffrierte Buchstabe erscheint, oder man beginnt bei H (bezw. C) und verfolgt ebenso die Vertikalreihe des Chiffrebuchstabens, natürlich unter steter Beachtung der oben erwähnten Bedeutung der Wahlzahl. —

Diese Methode ist allerdings etwas compliziert, gewährt aber auch desto grössere Sicherheit, die sich bis zur unmöglichen Entdeckung steigern kann. Daher ist sie für kleinere Mitteilungen entschieden zu empfehlen. —

Der unübersehbare Wert der obigen Tabelle für die geheime Correspondenz liegt zum grössten Teil in der Möglichkeit, eine Menge verschiedener geheimer Correspondenzmethoden zu construieren, die auch der Gefahr der Entdeckung durch Uneingeweihte zu widerstehen vermögen.

VII.

Chiffriermethode Napoleons I.

Auf dem gleichen Grundgedanken wie der Multiplikationschiffre (Methode VI) beruht die Chiffriermethode Napoleons I.

In der nachfolgenden Chiffretabelle ist jedes der untereinanderstehenden Alphabete durch je zwei Buchstaben der Wahllinie bezeichnet. Welches der verschiedenen Alphabete beim Chiffrieren jedesmal zur Anwendung kommt, geben die Buchstaben eines Wahlwortes an, die in ununterbrochener, nach Bedarf wiederholter Reihenfolge unter die Buchstaben der zu chiffrieren-

Digitized by Google

Wahllinie I.													Wahllinie II.
1	a	a	b	c	d	e	f	g	h	i	k	l	m	z
	b	n	o	p	q	r	s	t	u	v	w	x	z	x
2	c	b	c	d	e	f	g	h	i	k	l	m	n	w
	d	o	p	q	r	s	t	u	v	w	x	z	a	v
3	e	c	d	e	f	g	h	i	k	l	m	n	o	u
	f	p	q	r	s	t	u	v	w	a	b	x	z	t
4	g	l	m	n	o	p	q	r	s	t	u	v	w	s
	h	x	z	a	e	f	g	h	i	k	b	c	d	r
5	i	f	g	h	i	k	l	m	n	o	p	q	r	q
	k	l	d	e	b	a	z	x	w	v	u	t	s	p
6	l	o	p	q	r	s	t	u	v	w	x	z	a	o
	m	n	m	l	k	i	h	g	f	e	d	c	b	n
7	n	s	t	u	v	w	x	z	a	b	c	d	e	m
	o	r	q	p	o	n	m	l	k	i	h	g	f	l
8	p	z	a	b	c	d	e	f	g	h	i	k	l	k
	q	x	w	v	u	t	s	r	q	p	o	n	m	i
9	r	q	r	s	t	u	v	w	x	z	a	b	c	h
	s	p	o	n	m	l	k	i	h	g	f	e	d	g
10	t	h	i	k	l	m	n	o	p	q	r	s	t	f
	u	g	f	e	d	c	b	a	z	x	w	v	u	e
11	v	o	p	q	r	s	t	u	v	w	x	z	a	d
	w	g	h	i	k	l	m	n	f	e	d	b	c	c
12	x	r	s	t	u	v	w	x	z	a	b	c	d	b
	z	q	p	o	n	m	l	k	i	h	g	f	e	a

den Mitteilung geschrieben werden. In dem anzuwendenden Alphabete wird nun aber, abweichend von dem Multiplicationschiffre, jeweils der dem eigentlichen Chiffrebuchstaben gegenüberstehende Buchstabe benutzt.

Z. B. *h* im Alphabete a (oder b) der Wahllinie I wird chiffriert mit *u*; *s* im Alphabete t (oder u) mit *v* etc. (Ebenso umgekehrt v mit s).

Beispiel: Die Mitteilung: „Wann treffen wir uns“ soll chiffriert werden. Das Wahlwort sei: Marine;

Also: W a n n t r e f f e n w i r u n s
m a r i n e m a r i n e m a r i n

Digitized by Google

Der Buchstabe *w* im Alphabet m (Wahllinie I) ist durch den ihm gegenüberstehenden Buchstaben *e* zu ersetzen, *a* im Alphabet a durch *n* etc.

So erhält man: enswqewsafwkse.

Bei der Wahl des Wahlwortes muss man darauf bedacht sein, dass nicht wie im Alphabet (der Wahllinie) zwei Buchstaben aufeinander folgen, die nur den Gebrauch eines Alphabetes ermöglichten, z. B. das Wort „Feldkirch" lässt, trotzdem es neun Buchstaben hat, nur sieben Alphabete zur Anwendung übrig, weil *fe* und *ki* je ein Alphabet bezeichnen. Ebenso vermeide man Wörter mit Verdoppelungen z. B. „Pfeffer", welches Wort nur drei Alphabete zur Verwendung zulässt.

Bei der Dechiffrierung müssen die Buchstaben des Wahlwortes unter die der geheimen Mitteilung geschrieben werden, und genau wie oben geschieht die Versetzung der einzelnen Buchstaben:

Also: e n s w q e etc.
m a r i n e etc.

e im Alphabet m ist zu ersetzen mit w
n „ „ a „ „ „ „ a
s „ „ r „ „ „ „ n
w „ „ i „ „ „ „ n etc.

Die Vorzüge dieser Methode gegenüber derjenigen von Julius Caesar liegen offen da: bei jedem Buchstaben wird ein anderes Alphabet angewandt, sodass gleiche Buchstaben eines Wortes jeweils durch verschiedene Chiffrebuchstaben ersetzt werden. — Die Methode an und für sich ist sehr bequem anzuwenden und lässt sich auch als Versetzungsmethode gebrauchen; sie kann aber auch ganz vorteilhaft als selbständige Methode mit einer anderen Versetzungsweise verbunden werden. — Von den bekannten — oben erwähnten — Kunstgriffen lassen sich auch hier einige verwenden. —

Verabredetes Wechseln zwischen Wahllinie I und II bildet die Grundlage vieler Variationen. —

Statt eines Wahlwortes lässt sich auch ebensogut eine Wahlzahl vereinbaren und gebrauchen (Vergleiche Methode VI, 4).

Digitized by Google

VIII.

Methode durch Bildung neuer Wörter.

Eine gute, sehr empfehlenswerte Versetzungsmethode ist diese:

Auf eine noch näher zu besprechende Weise werden neue Wörter gebildet durch Zusammenstellung verschiedener aus der ganzen Mitteilung herausgenommener Buchstaben; es werden wohl die Buchstaben der zu chiffrierenden Mitteilung nacheinander in verschiedene Colonnen eingetragen; aber bei dem neu entstandenen Chiffreworte steht z. B. der 3., 21., 39., 57. etc. Buchstabe der Mitteilung in Klarschrift nebeneinander.

Das Verfahren bei dieser Zusammenstellung der Buchstaben ist nun folgendes:

Zunächst wähle man die Art der Versetzung, indem man mit 3, 4, 5 . . . . Ziffern eine Anzahl (Ziffern-) Gruppen bildet und sie nach genauer Vereinbarung in einer Colonne untereinander schreibt, wie die Figur anzeigt.

Es seien z. B. aus den vier Ziffern 1, 2, 3, 4 fünf verschiedene Gruppen gebildet: 2 4 1 3, 3 1 2 4, 2 1 3 4, 4 3 1 2, 3 2 1 4, die untereinander zu schreiben sind.

Die Mitteilung: „Ich nehme an deinem Verluste innig teil und troeste dich mit dem Wunsche einer gluecklicheren Zukunft“

	1	2	3	4	1. Rub.	2. R.	3. R.	4. R.
I.	2	4	1	3	c s t i k	n e d e n	i u s e u	h t e n u
II.	3	1	2	4	m n h l a	e i i r f	h n c g t	e i m u b
III.	2	1	3	4	n t t c c	a g i e d	d e d k e	e i e l f
IV.	4	3	1	2	m d n e g	e n u h h	i l m i i	n u w c k
V.	3	2	1	4	r o h n l	e r c e m	v t s r n	l e e z o

wird nun auf folgende Weise in die übrigen Felder eingetragen:

Vorerst schreibt man die Ziffern 1—4 in regelmässiger Reihenfolge unter die einzelnen Buchstaben der Mitteilung:

i c h n e h m e a n d e i n e m v e r l u s t e etc.
1 2 3 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2 3 4 etc.

Die Zahlen in der vorderen Rubrik der Figur ordnen die Reihenfolge der Chiffrebuchstaben, indem ihre einzelnen Ziffern durch ihren natürlichen Wert die „zeitliche“, durch ihre Stellung aber die „örtliche“ Reihenfolge bedingen, d. h. an der Stelle, wo die kleinste Ziffer (d. i. *1*) steht, beginnt das Versetzungsverfahren in jeder Zeile

Digitized by Google

(Horizontallinie), und wo die grösste Ziffer (d. i. *4*) steht, endigt es. Der erste Buchstabe *i* wird, da in der ersten Horizontallinie die Ziffer *1* (der Zahl 2 4 1 3) an dritter Stelle steht, in die Rubrik 3 gesetzt werden müssen; der 2. Buchstabe *c*, wird, da *2* an der ersten Stelle (der Zahl 2 4 1 3) steht, in die Rubrik *1* einzutragen sein; der fünfte Buchstabe (der Mitteilung) *e*, der wieder mit *1* bezeichnet ist, wird, da *1* in der zweiten Zahl (3 1 2 4) an zweiter Stelle steht, in die Rubrik *2* eingetragen; der sechste Buchstabe h_2 wird sodann in der gleichen Linie in die Rubrik 3 eingetragen, da die ihn bezeichnende Ziffer 2 an der dritten Stelle steht. So wird das Verfahren fortgesetzt, bis auch die fünfte Horizontallinie erledigt ist, worauf dann mit dem 21. Buchstaben u_1 wieder in der ersten Horizontallinie begonnen wird, der aus dem gleichen Grunde wie der allererste Buchstabe *i* in die Rubrik 3 eingetragen wird *). — Nachdem der letzte Buchstabe *t* an seine richtige Stelle geschrieben ist, füllt man die übrigen Rubriken mit beliebigen Buchstaben in der Weise aus, das in jeder Rubrik je fünf Buchstaben untereinander stehen, worauf die zu übersendende Mitteilung dann folgende Form erhält:

cstik neden iuseu htenu mnhla eiirf etc.

Ein Vorzug dieser Methode ist es, dass man bei jeder neuen Mitteilung mit der Anzahl der Ziffern ohne jedesmalige Verabredung wechseln kann; allerdings muss man es dem Empfänger der Mitteilung irgendwie erkennbar machen, ob man 3, 4, 5, 6 etc. Ziffern zur Bildung der Gruppen von Zahlen und zur Versetzung der Buchstaben anwendete: Dies geschieht entweder dadurch, dass man die betreffende Zahl oder ein dieser entsprechendes Vieleck etc. der geheimen Mitteilung voransetzt; oder man deutet dies so an, dass man nach der entsprechenden Anzahl von Buchstaben der Chiffreschrift (am Anfange derselben) eine Unterbrechung eintreten lässt, z. B. in obigem Falle: csti k neden iuseu etc.

oder: 4 cstik neden iuseu etc. —

oder: □ cstik neden iuseu etc. —

Ob man nun 3, 4, 5 . . . . Ziffern anwenden will, die Zahlengruppen sowie deren Aufeinanderfolge müssen ein für alle Mal verabredet sein. —

Beim Dechiffrieren hat man zunächst auf die angedeutete Anzahl der Ziffern zu achten, wonach sich auch die Anzahl der Rubriken richtet, die man nach der obigen Figur bildet. Nachdem

*) Vgl. die Aehnlichkeit dieser Chiffrierart mit Methode XVI, I. Abschnitt.

Digitized by Google

die verabredeten Zahlengruppen (vor der ersten Rubrik) untereinander geschrieben sind, setzt man — wie die Figur zeigt — die einzelnen Wörter der Chiffreschrift in die leeren Felder ein.

Das Aufsuchen der Buchstaben der Klarschrift geht dann in ähnlicher Weise vor sich, wie das Einsetzen der Buchstaben der Chiffreschrift *). —

IX.

Methode Richelieu's.

Wie in der vorigen Methode die ganze Mitteilung als eine einzige Gruppe von Buchstaben behandelt wird, kann aber auch die ganze Mitteilung in mehrere Gruppen zerlegt werden, und die Buchstaben jeder Gruppe können nach einer verabredeten Ordnung versetzt werden (Richelieu's Versetzungsmethode).

In dem nachstehenden Beispiele sind Gruppen von *11* Buchstaben gebildet, die verabredete Versetzungsordnung der einzelnen Buchstaben(=Wahlzahl) wäre beispielsweise diese:

3 8 2 7 1 9 11 5 10 4 6.

Es soll z. B. die Mitteilung:

„Binnen einiger Tage wird dir ein Brief meine Ankunft melden“ auf diese Art chiffriert werden:

	I.										II.															
1	2	3	4	5	6	7	8	9	10	11	1	2	3	4	5	6	7	8	9	10	11	1	2	3	4	5
b	i	n	n	e	n	e	i	n	i	g	e	r	t	a	g	e	w	i	r	d	d	i	r	e	i	n
3	8	2	7	1	9	11	5	10	4	6	3	8	2	7	1	9	11	5	10	4	6	3	8	2	7	1

etc.

Jetzt werden zuerst die Buchstaben der Gruppe I versetzt, indem jeweils durch die unter ihnen stehende Zahl der Versetzungsbuchstabe, der die gleiche Zahl über sich stehen hat, erkennbar gemacht ist.

Also:

der erste Buchstabe *b* wird durch den 3. Buchstaben (*n*) der gleichen Gruppe ersetzt,
„ zweite „ *i* „ „ „ 8. „ (*i*) „ „ „ „
„ dritte „ *n* „ „ „ 2. „ (*i*) „ „ „ „
„ elfte „ *g* „ „ „ 6. „ (*n*) „ „ „ „ .—

Sodann wird die Gruppe II etc. auf gleiche Weise behandelt. —

*) Vgl. hierzu III. Abschnitt, I. Capitel dieser Darstellung.

Digitized by Google

Die Chiffreschrift wird lauten:

niiebngeinntirwerdgdaee etc.

Man wird bemerken, dass z. B. der Buchstabe *e* stets durch einen anderen Buchstaben ausgedrückt ist, sodass nicht erst der Mangel der Methode I (dieses Abschnittes) beseitigt werden muss; ebenso kann man die Chiffreschrift in ganz beliebige Gruppen teilen; diese Vorteile lassen die Methode als eine durchaus empfehlenswerte Versetzungsmethode erscheinen. —

Mit dem Umfang der Zahlen kann man — wie in der vorigen Methode — auch nach Belieben wechseln, natürlich unter den gleichen Bedingungen wie dort. —

Beim Dechiffrieren hat man nur die verabredete Ordnung der Zahlen unter die Buchstaben der einzelnen Gruppen zu schreiben,

I.

	n	i	i	e	b	n	g	e	i	n	n	t	i	r	w	e	r	d	g
also:	3	8	2	7	1	9	11	5	10	4	6	3	8	2	7	1	9	11	5

} etc.

nach arithmetischer Ordnung aneinandergereiht:

b	i	n	n	e	n	e	i	n	i	g	e	r	t	
1	2	3	4	5	6	7	8	9	10	11	1	2	3	

} etc.

I.

X.

Der Netz- oder Gitterchiffre.

In Folgendem will ich den sogenannten Netz- oder Gitterchiffre besprechen. Seine Grundidee ist schon sehr alt und reicht bis in das 16. Jahrhundert zurück. Im Laufe der Zeit hat er allerdings manche Verbesserungen erlebt; so durch C. F. Hindenburg (1796), Maurice de Prasse (1799), Martens (1851) und in neuerer Zeit durch A. L. Flamm und E. B. Fleissner (1881), dessen „neue Patronen-Geheimschrift“ ich weiter unten noch besprechen werde *). —

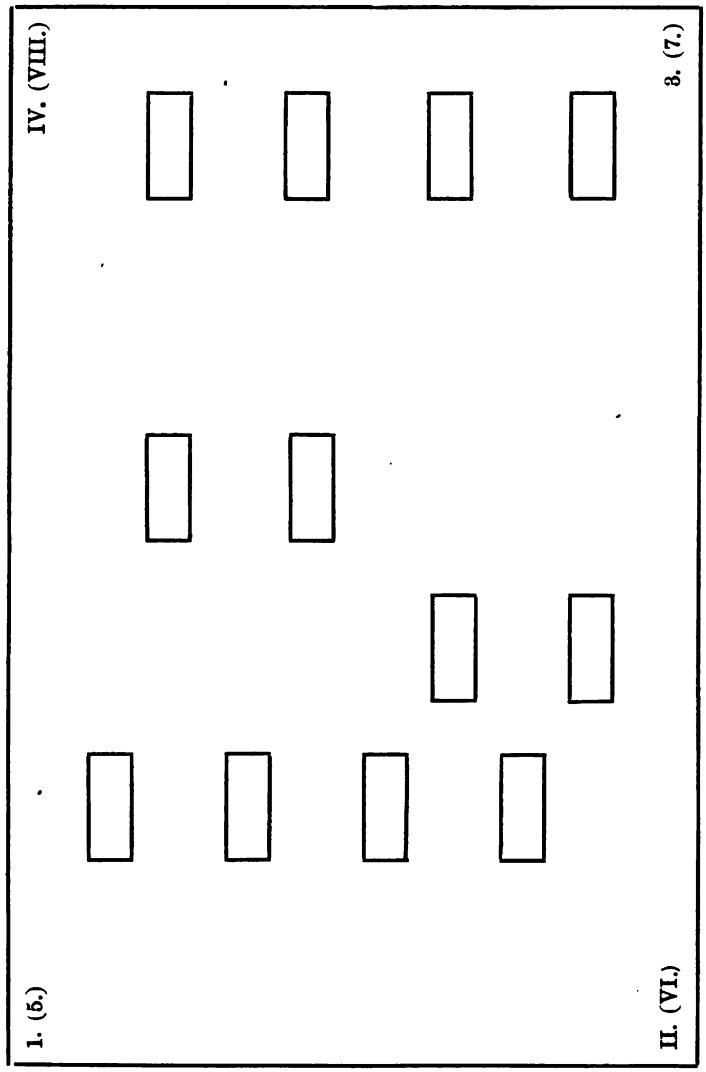
Als Schlüssel gebraucht man eine eigenartig durchlöcherte Karte (sog. „Netz“ oder „Patrone“), die so eingerichtet ist, dass die Buchstaben oder Wörter der Mitteilung, durch diese Löcher

*) Vgl. die nachfolgende Methode XI.

Digitized by Google

auf eine darunterliegende Karte geschrieben, aus ihrem Zusammenhange gebracht und so untereinander gemischt werden, dass nach Wegnahme der Patrone die Mitteilung chiffriert und unleserlich ist.

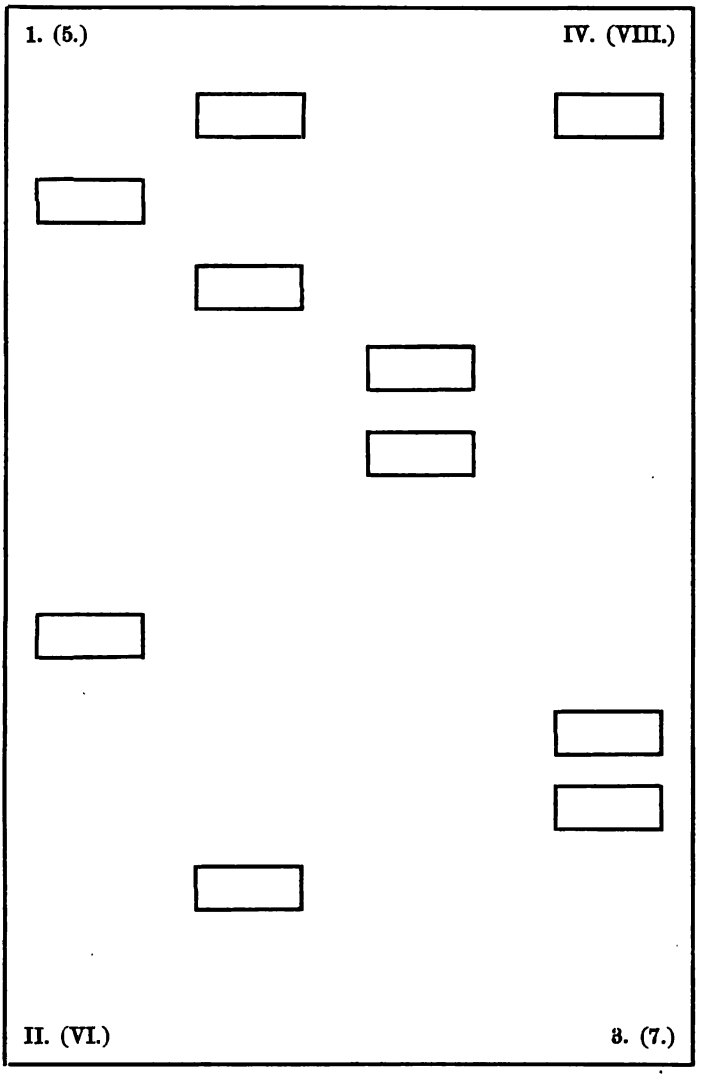
Um bequem eine Postkarte für eine nach dieser Chiffremethode zu chiffrierende Mitteilung benutzen zu können, konstruierte ich zwei „Patronen“ in dem natürlichen Format unserer Postkarte, wobei ich auf eine etwaige Vorliebe, der Breite oder Länge nach die Karte zu beschreiben, Rücksicht nahm. —



Figur 1.

Digitized by Google

Figur 2.



Die Herstellung einer so durchlöcherten „Patrone“ geschieht einfach dadurch, dass man von Fig. 1 oder 2 durch Nadelstiche die Rechtecke auf eine darunterliegende (verbrauchte) Postkarte überträgt und dann ausschneidet.

Die Ziffern in den Ecken der „Patrone“ nummerieren die acht verschiedenen Möglichkeiten, die „Patrone“ auf die zu beschreibende Karte zu legen. Die Reihenfolge der verschiedenen

Digitized by Google

Auflegearten kann beliebig verabredet werden. Hier stehen die Ziffern 1. (5.), 3. (7.) auf der Vorderseite, II. (VI.), IV. (VIII) auf der Rückseite der „Patrone". — Eine so präparierte „Patrone" verwendet der Absender beim Schreiben und der Empfänger beim Lesen der Mitteilung.

Die Anwendung der „Patrone" ist nun folgende:

Der Schreiber legt dieselbe auf die zu beschreibende (Post-) Karte, indem er nach links oben die Ziffer *I* dreht; nun füllt er die Löcher der Reihe nach von oben nach unten aus mit der fortlaufenden Mitteilung; beim letzten Loche angelangt, dreht er die „Patrone" so um, dass links oben die Ziffer II zu stehen kommt füllt dann wie vorher die Löcher der Reihe nach aus, wendet schliesslich die „Patrone" so, dass links oben die Ziffer 3 und dann IV erscheint. — Sollte bis jetzt die Mitteilung noch nicht zu Ende sein, so kann man genau dieselbe Manipulation noch einmal von Anfang beginnen, aber stets mit der „Patrone" (bei jeder Drehung) eine Zeile tiefer rückend, um so einen neuen freien Raum unter dem zuerst Geschriebenen zu gewinnen. —

Es ist ratsam in jedes Loch nur ein Wort zu schreiben (eventuell auch zwei kleine); jedenfalls vermeide man es aber, wegen unzureichenden Raumes auffallende Worttrennungen vorzunehmen. —

Die bis jetzt besprochenen Versetzungsmethoden bezweckten alle eine Versetzung der einzelnen Buchstaben einer Mitteilung; der Netzchiffre versetzt aber ganze Wörter einer Mitteilung, so dass dieselben ohne jeglichen Zusammenhang neben- und untereinanderstehen, weshalb es auch nicht leicht ist, den Sinn der Mitteilung zu erraten. Natürlich bietet diese Methode, so wie sie jetzt vorliegt, nicht völlige Sicherheit des Geheimnisses, was aber durch Variationen erreichbar ist.

Mehr Sicherheit bietet der Netzchiffre schon dadurch, dass man je 1, 2, 3 etc. Buchstaben in ein Loch setzt und den etwa übrigbleibenden Raum mit Nieten ausfüllt; so wird der Netzchiffre zu einer Versetzungsmethode im eigentlichen Sinne des Wortes und eignet sich als solche sehr vorteilhaft zum Chiffrieren einer Mitteilung *). —

*) Eine genaue Zeichnung nach obiger Fig. 1 oder 2 lässt sich auch wie ein Linienblatt benützen, indem die Buchstabengruppen (bezw. die Wörter) in die durchscheinenden (gezeichneten oder ausgeschnittenen) Rechtecke geschrieben werden, wobei allerdings eine Postkarte nicht verwendbar ist. —

Digitized by Google

Ferner kann man die bereits nach einer anderen Methode chiffrierte Mitteilung durch den Netzchiffre vorteilhaft „verwirren" (d. h. „versetzen"), in dem man beliebige Buchstabengruppen in die einzelnen Löcher setzt.

Kurzum der Netzchiffre eignet sich sehr gut als Versetzungsmethode und bietet bei der Verabredung dem Correspondenten eine Menge Variationen, weshalb diese Methode recht zu empfehlen ist. —

Es besteht nun auch eine scheinbar vorzügliche Variation, besonders weil ihre Anwendung dem Unberufenen gegenüber keinen Verdacht einer geheimen Mitteilung erregen soll. Auf die Mängel dieser Variation werde ich aber speziell im dritten Abschnitt (Cap. II.) noch zurückkommen. —

Die Idee dieser Variation ist folgende:

Beliebig verabredete Löcher einer Auflegeart der Patrone werden mit den Wörtern der geheimen Mitteilung in natürlicher Reihenfolge ausgefüllt, (wobei aber die Schreibart ihre volle Geltung behalten muss, d. h. Substantiva und Eigennamen sind gross zu schreiben). — Darauf wird die Patrone entfernt, und die zur Trägerin der Mitteilung dienende Karte wird vom Anfang an mit einer gleichgiltigen, unwichtigen Mitteilung beschrieben, wobei aber die in unregelmässigem Abstand voneinander stehenden Wörter der (bereits niedergeschriebenen) geheimen Mitteilung jeweils in den Zusammenhang der unwichtigen Mitteilung hineinzuflechten sind, sobald man auf ein solches Wort stösst. Also die zuerst geschriebenen Wörter (der geheimen Mitteilung) dürfen im Zusammenhang mit den anderen Wörtern (der unwichtigen Mitteilung) absolut nicht den Sinn der allgemeinen Mitteilung stören. Eine so beschriebene Karte wird dem Empfänger beim Dechiffrieren nicht die geringste Schwierigkeit bieten, da er nur seine Patrone aufzulegen braucht und nach der Verabredung die einzelnen Wörter der geheimen Mitteilung abliest. — Bedeutend schwieriger hat es aber der Schreiber der Mitteilung, da es durchaus nicht so leicht und einfach ist, bei einer Mitteilung unauffälligen Inhaltes eine Anzahl Wörter an genaubestimmter Stelle in den Zusammenhang der ganzen Mitteilung zu bringen. Je grösser nun die Anzahl der Wörter (der geheimen Mitteilung) ist, desto schwieriger ist es eben auch, sie im Zusammenhang der allgemeinen Mitteilung zu verbergen.

Digitized by Google

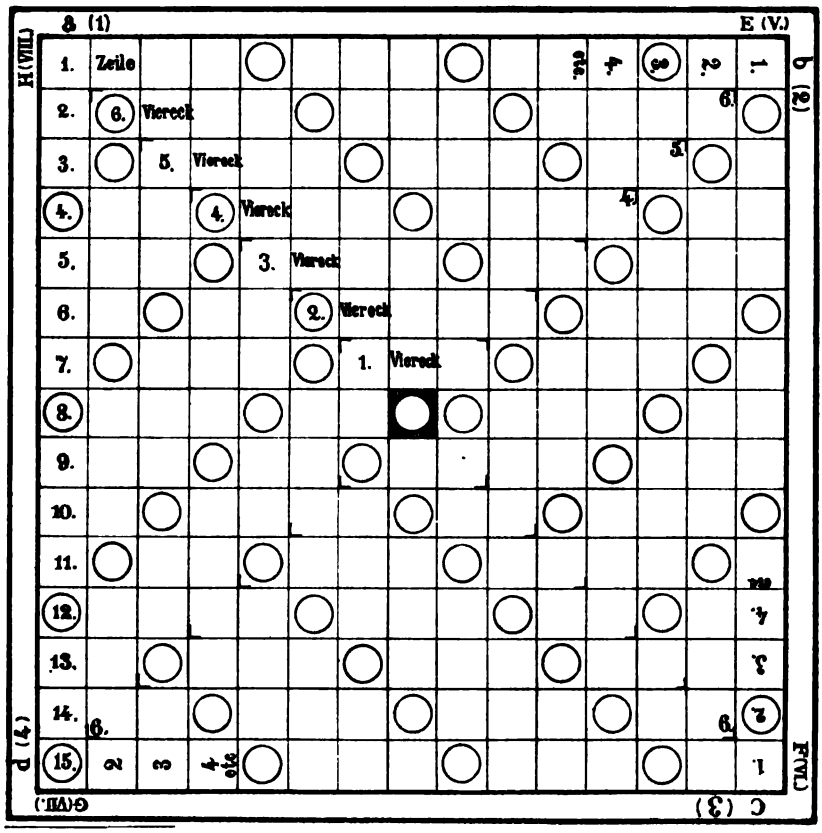
Da diese Variation sich nur für ganz kurze (geheime) Mitteilungen eignen könnte und die eben erwähnte Art ihrer Anwendung manche verräterische Mängel in sich einschliesst, wird sich ein Gebrauch dieser Variation nicht empfehlen lassen *). —

XI.

Fleissners neue Patronengeheimschrift.

Auf dem gleichen Prinzip wie der Netz- oder Gitterchiffre beruht Fleissners „neue Patronengeheimschrift", die eine Anzahl — wenn auch complizierte — Variationen, mit grossem Vorteil anwendbar, gestattet. —

Nachstehende Figur stellt die „Patrone" zu Fleissners Geheimschrift dar; über die Anwendungsweise gilt das bei dem Netzchiffre Gesagte; aber hier werden in die Löcher nur einzelne Buchstaben oder Ziffern eingezeichnet. —



*) Vgl. hierzu III. Abschnitt, II. Capitel dieser Darstellung.

Digitized by Google

Bei Anfertigung einer solchen „Patrone", die übrigens auch grösser oder kleiner gewählt werden kann, hat man das quadratische Papier (Carton) in lauter kleine Quadrate einzuteilen, worauf dann die obiger Figur entsprechenden Stellen markiert und mit einem Locheisen ausgestanzt werden. Hierauf werden die nötigen Vermerke auf der Patrone angebracht, besonders die Nummerierung der acht Auflegearten. In der Figur sollen die Bezeichnungen *a* (1), *b* (2), *c* (3), *d* (4) auf der Vorderseite, *E* (V), *F* (VI), *G* (VII), *H* (VIII) auf der entsprechenden Rückseite der „Patrone" stehen. — Das in der Mitte der „Patrone" liegende (schraffierte) Quadrat soll bei der Anwendung derselben stets zur Einzeichnung desjenigen (am Rand der Patrone stehenden) Buchstabens (oder Ziffer) benutzt werden, mit welchem man die Patrone aufzulegen begonnen hat. —

Will man eine kleinere Mitteilung auf diese Art chiffrieren, so genügt es, nur einen Teil der „Patrone dabei zu benützen; zu diesem Zwecke dient der Vermerk auf der „Patrone" 1. bis 6. Viereck, wobei dann jeweils der äussere Rand unbenutzt bleibt; ferner kann man bei kleinen Mitteilungen nur gewisse Zeilen zur Chiffrierung anwenden, z. B. die 1. bis 8. Zeile (sh. Figur), wobei die 9. bis 15. Zeile bei jeder Umdrehung der „Patrone" unbenutzt bleiben; die chiffrierte Mitteilung wird sich in diesem Falle nur auf die obere Hälfte der „Patrone" erstrecken. Ebenso kann bloss die untere Hälfte der „Patrone" (also die 8. bis 15. Zeile) benutzt werden, oder die mittlere Hälfte d. i. z. B. 3. bis 8., 9., 10. etc. Zeile. Jedenfalls soll aber stets die 8. Zeile dabei benutzt werden, um im schraffierten Loche der „Patrone" anzeigen zu können, mit welcher Seite man das Auflegen begann. Man sieht jetzt schon, welche Vorteile diese Patrone bei der Wahl ihrer Anwendung und Benutzung bietet. —

Ich muss hier noch eine besondere Variation dieser Methode erwähnen. Um unter die geltenden Chiffrebuchstaben andere irreführende Buchstaben (Nieten) zu mischen, schlägt Fleissner vor, die „Patrone" ganz beliebig aufzulegen und die Löcher mit gleichgiltigen Buchstaben von Anfang bis zum Ende auszufüllen; dabei muss dem Empfänger im Mittelloch angedeutet werden, welche Auflegeart beim Niederschreiben der Nieten gewählt wurde; sodann muss durch einen zweiten Buchstaben (oder Ziffer) im Mittelloch angezeigt werden, mit welcher Auflegeart der Schreiber begonnen hat, die Mitteilung nach der bekannten Weise in die Löcher einzutragen. — Bei nachstehender Chiffrierung

Digitized by Google

f p t a v a b
e c d s a h e
p r r i e w e
a n d fa h f r
g o r h r h i
t e k e o g d
i l e g e m u

wurden die 3 inneren Vierecke (das 1. 2. und 3.) der „Patrone“ (siehe Figur) gebraucht, und zwar wurden — wie die erste Bezeichnung im Mittelloch (*f*) anzeigt — zuerst alle Löcher der Auflegeart *f* mit gleichgiltigen Buchstaben (a, b, c, d . . . . m) ausgefüllt, sodann wurde mit der Auflegeart *a* — wie die zweite Bezeichnung im Mittelloch angibt — begonnen, indem die Buchstaben der Mitteilung nacheinander in die noch leeren Löcher eingezeichnet wurden. Es wurden dann ebenso die noch leeren Löcher der Auflegeart *b, c* und *d* ausgefüllt, und in die beiden letzten leergebliebenen Löcher wurden die nichtsbedeutenden Buchstaben *n* und *o* eingezeichnet.

Legt man nun, dieser Erklärung entsprechend, eine „Patrone“ nach obigem Muster auf die Chiffreschrift, so erhält man nach Entfernung der Nieten a, b, c, d . . . m (der Auflegeart *f*) die Mitteilung:

„Verwahre die Papiere gut, es droht Gefahr“.

Beim Einzeichnen der Buchstaben der Mitteilung sind natürlich Interpunktionszeichen und Majuskeln — wie bei anderen Chiffreschriften — sorgfältig zu vermeiden. —

Der Empfänger der geheimen Mitteilung, der die gleiche „Patrone“ wie der Schreiber besitzen muss, kann aber auch die Chiffreschrift entziffern, wenn sie folgende weniger auffallende Form hat:

fptavabecdsaheprrieweand fa hfrgorh etc.

Denn wenn der Empfänger durch die Verabredung weiss, welchen Teil der „Patrone“ der Schreiber gebrauchte, so wird er leicht nach dem Mass seiner „Patrone“ die Quadrate jenes Teiles herstellen und die Chiffrebuchstaben der Reihe nach in diese Quadrate einzeichnen können. Jedenfalls sind bei dieser Form der Chiffreschrift dem Empfänger durch irgend welches Zeichen die Buchstaben (oder Ziffern) des Mittelloches der „Patrone“ erkennbar zu machen (In obigem Beispiel durch Isolierung der beiden Buchstaben *fa*). —

Digitized by Google

Es wird übrigens auch nicht schwer sein, bei jeder neuen Mitteilung den beliebig gewählten Teil der „Patrone“ dem Empfänger irgendwie anzudeuten, sodass ohne vorherige Verabredung jederzeit mit den Teilen der „Patrone“, wie auch mit den Auflegearten gewechselt werden kann, was von grossem Vorteil für die Sicherheit des Geheimnisses ist. —

Um Nieten in diese Art der Geheimschrift einzuschalten, hat Fleissner noch eine besondere Methode angegeben. Er empfiehlt nämlich zu diesem Zwecke die Construction sogenannter Complicanten, d. h. „Patronen“, die in Grösse und Einteilung (in kleine Quadrate) der eigentlichen „Patrone“ genau entsprechen müssen, aber mit dem Unterschiede, dass die Löcher in denselben ganz nach Belieben angebracht werden. Ehe nun die eigentliche Chiffrierung den Mitteilung vorgenommen wird, wird zuerst der Complicant auf eine einzige, dem Empfänger aber anzudeutende Art aufgelegt, und die einzelnen Löcher desselben werden mit gleichgiltigen Buchstaben ausgefüllt; hierauf geht die Chiffrierung mit der eigentlichen „Chiffrierpatrone“ auf die oben erörterte Weise vor sich. Es ist diese Variation also ganz ähnlich wie die zuerst erwähnte Art der Einschaltung von Nieten und hat daher keine besondere Beachtung zu beanspruchen. —

Fleissner gibt in seinem Werke S. 92 ff genau die Herstellungsweise von „Patronen“ an und stellt einige „Patronen“- und Complicantenmuster dar, die alle anzuführen über den Rahmen meiner Darstellung hinausginge; nur sei noch hier bemerkt, dass „Patronen“, die auf einem grösseren Netze construiert werden, eine bedeutend grössere Sicherheit gewähren als solche auf zu kleinem Netze construierte. —

Man muss die Vorzüge dieser „neuen Patronengeheimschrift“ in jeder Hinsicht anerkennen; der Hauptvorzug ist eben der, dass man mit ihr eine Menge Variationen vornehmen kann, die alle nur auf der Verabredung der beiden Correspondenten beruhen. —

Sowohl als selbstständige Geheimschrift, wie auch als Versetzungsmethode leistet sie gute Dienste. Sie lässt sich auch mit Leichtigkeit mit anderen Geheimschriftmethoden verbinden, sodass sie zur Undurchdringlichkeit des Geheimnisses vieles beiträgt. Vor allem will ich die Verbindung der hebräischen und chinesischen Methode, sowie die Verbindung der Methode im Zickzack und in der Diagonale *) mit der Patronengeheimschrift erwähnen, d. h. jede dieser 4 Methoden ist gleichzeitig bei der Chiffrierung mit der

*) Siehe oben diese Methoden.

Digitized by Google

„Patrone“ anwendbar, sodass ausser den Auflegearten auch noch die Reihenfolge der einzelnen Löcher modifiziert werden kann. —

Noch ein anderer grosser Vorteil dieser Methode ist der, dass man dieselbe zur Chiffrierung jeder Mitteilung — ohne Unterschied der Länge oder Kürze — gebrauchen kann.

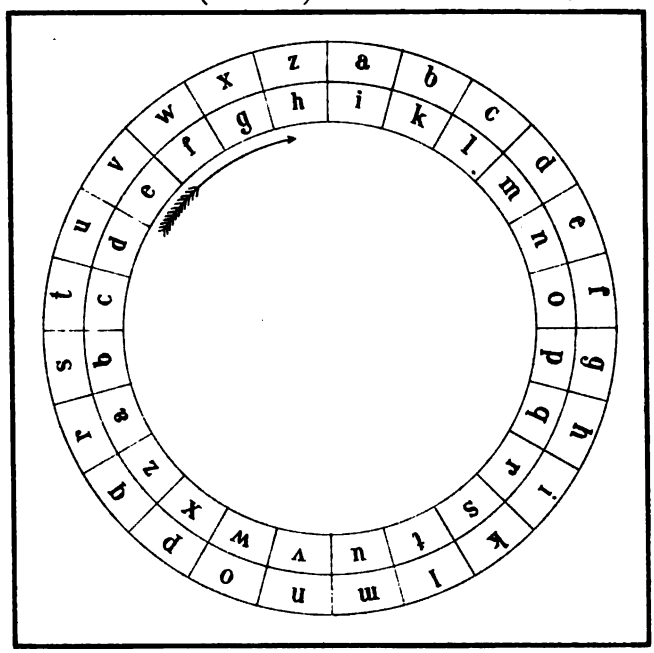
Wie man bei kurzen Mitteilungen, verfahren kann, wurde bereits angegeben; bei längeren Mitteilungen, die nach der 7. bezw. 8. Auflegung der Patrone noch nicht ganz chiffriert ist, kann man die Patrone, das Verfahren von neuem beginnend, direct an die letzte (15.) Zeile der bereits chiffrierten Mitteilung anlegen und nach Bedarf weitere Teile der „Patrone“ benützen *). —

XII.

Der Circularscheibenchiffre.

1. Auf dem Princip, mehrere Alphabete bei einer Chiffrierung anwenden zu können, beruht auch der Circularscheibenchiffre oder „the revolving dial cipher“ (nach Schooling).

Die Circularscheibe besteht aus zwei kreisförmigen Papier- oder Cartonscheiben, die im Mittelpunkt so mit einander verbunden sind, dass die innere (kleinere) Scheibe drehbar ist.



*) Vgl. III. Abschnitt, I. Capitel dieser Darstellung.

Digitized by Google

Das innere Alphabet ist also der Rand der inneren drehbaren Scheibe, das äussere Alphabet der Rand der äusseren unbeweglichen Scheibe.

Will man nun mit Hilfe einer solchen Circularscheibe eine geheime Mitteilung chiffrieren, so richtet man nach Verabredung irgend einen Buchstaben des inneren Alphabetes auf *a* des äusseren Alphabetes, (in der Figur *a i*); sodann ersetzt man die Buchstaben der zu chiffrierenden Mitteilung, die auf dem Rand der äusseren Scheibe zu suchen sind, durch die ihnen entsprechenden Buchstaben der inneren Scheibe. Um nun ein anderes Alphabet anwenden zu können, dreht man einfach die innere Scheibe nach einer verabredeten Richtung und deutet die Anzahl der übersprungenen Felder bei der weiteren Chiffrierung an. So kann man innerhalb derselben Mitteilung nach Belieben mit dem Alphabet wechseln, ohne vorherige Verständigung seines Correspondenten, was ein besonderer Vorzug dieser Methode ist. Uebrigens kann auch die erste „Einstellung" der inneren Scheibe ohne vorherige Verabredung beliebig gewählt werden, wenn man der chiffrierten Mitteilung den einem bestimmten Buchstaben (z. B. *a*) gegenüberstehenden Buchstaben (der Innenscheibe) voransetzt. Also an Variationen bei der Anwendung der Circularscheibe fehlt es nicht.

Wie bei den übrigen Methoden, so soll auch hier des besseren Verständnisses halber ein Beispiel aufgezeichnet werden.

Die Mitteilung: „Antwort kam zu spät" bekäme z. B. folgende Form: ai ivcfwac 3 pfr 2 cx vsdhw.

oder ai ivcfwac af pfr ad cx vsdhw.

ai (bezw. 1) zeigt die erste „Einstellung" der inneren Scheibe an, 3 (= af) zeigt an, dass die Innenscheibe um drei Felder von links nach rechts weiter gedreht wurde, 2 (= ad) deutet die Weiterdrehung der Innenseite um zwei Felder (im ganzen also jetzt um fünf Felder) an. — So kann man natürlich an jeder beliebigen Stelle eines Wortes eine Drehung der Scheibe vornehmen und anzeigen.

Der Circularscheibenchiffre leistet als selbständige Geheimschriftmethode, sowie auch als Versetzungsmethode vorzügliche Dienste bei der Chiffrierung von Mitteilungen.

---

2. Ganz ähnlich wie die vorige Methode ist der Leiterchiffre;*) seine Anwendungsweise ist genau wie die des Circularscheibenchiffres, nur erheischt seine eigenartige Construction eine

*) Zwei ähnliche (verschiebbare Zahlen-) Chiffres finden sich bei Fleissner S. 38 ff.

Digitized by Google

etwas verschiedene Aufsuchung der Chiffrebuchstaben, was aus nachstehenden Figuren leicht ersichtlich ist.

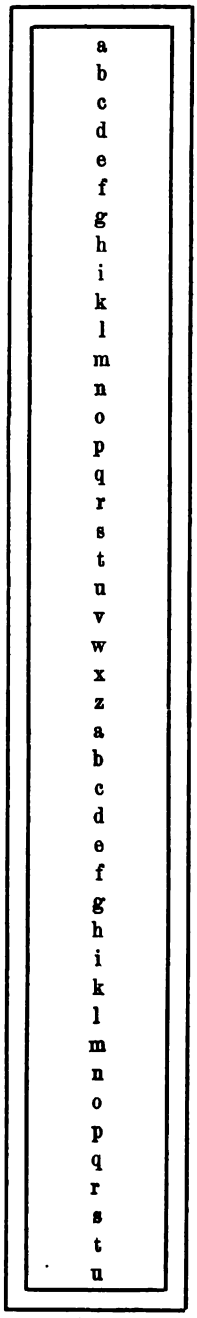


Fig. a.

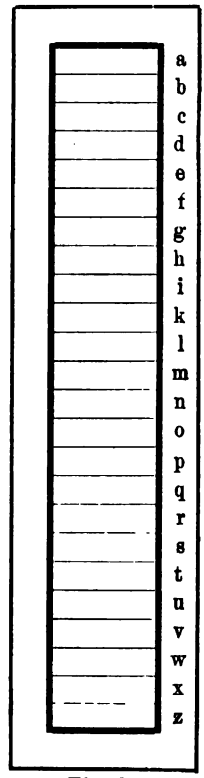


Fig. b.

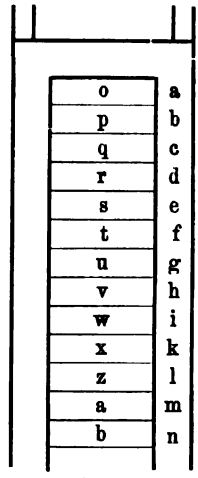


Fig. c.

Wie bei der Circularscheibe durch Drehen der inneren Scheibe stets ein neues Alphabet zu erhalten ist, so erzielt man beim Leiterchiffre das gleiche Resultat, indem man den einen durchlöcherten Papier- (oder Carton-)streifen (Fig. b) auf dem anderen (Fig. a) auf- und abbewegt. Ueber die verschiedenen Auflegearten und deren Bezeichnung in der chiffrierten Mitteilung gilt genau das oben über die Art der „Einstellung" der Innenscheibe Gesagte. Legt man z. B. den mit 24 rechteckigen Ausschnitten versehenen Streifen (Fig. b) auf den anderen Streifen (Fig. a) derart auf, dass in dem links von *a* (Fig. b) stehenden Rechtecke der Buchstabe *o* erscheint (Fig. c), so kann man die Mitteilung:

„Erwarte dich sicher"

z. B. so chiffrieren, dass man beim 2. Wort (dich) 4 Felder und beim 3. Wort (sicher) nochmals 2 Felder (zusammen also 6 Felder) höher rückt;

Also:

ao sflofhs 4 nsmr 2 aqkpmz

oder:

ao sflofhs ak nsmr ah aqkpmz

Digitized by Google

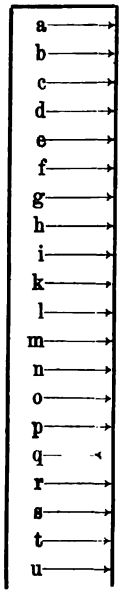


Fig. d.

Bezüglich der Variationen in der Anwendung des Leiterchiffres habe ich nichts mehr hinzuzufügen, sondern verweise auf das oben bei dem Circularscheibenchiffre Gesagte.

Nur will ich noch auf ein bequemeres Mittel, diese Methode anzuwenden, aufmerksam machen. Die Herstellung des verschiebbaren Streifens, wie ihn Fig. b zeigt, dürfte etwas umständlich sein; hingegen ist die Herstellung eines gewöhnlichen Papierstreifens nach Fig. d äusserst einfach; die Auf- und Abbewegung desselben zwecks Aufsuchens der Chiffrebuchstaben geschieht auf dem linken Rand des Streifens (Fig. a), sodass die Pfeilspitzen jeweils auf den zu suchenden Buchstaben gerichtet sein werden.

XIII.

Bacon's Vermehrungschiffre.

1. Ein Vermehrungschiffre, in welchem ein Buchstabe jeweils durch mehr als 1 Chiffrebuchstabe ersetzt wird, ist die Geheimschriftmethode des englischen Staatsmannes Francis Bacon (1561—1626). Seine Methode beruht darauf, dass durch Variation zweier beliebiger Buchstaben, die jeweils z. B. eine fünfgliederige Gruppen bilden (z. B. gggii), jeder einzelne Buchstabe des Alphabetes ausgedrückt wird.

Wählt man beispielsweise die beiden Buchstaben *i* und *g*, so lassen sich durch die erwähnte Variation derselben die 24 Buchstaben des Alphabets folgendermassen ausdrücken:

a	b	c	d	e	f	g	h	i
gigig	giggg	gigii	giigg	ggiii	giiii	giigi	giiig	iggig

k	l	m	n	o	p	q	r
igggg	igggi	iggii	igigg	igiii	igigi	igiig	iigig

s	t	u	v	w	x	z
iiggg	iiggi	iiigg	gggii	iiigi	iiiii	iiiig

Bei diesen Variationen ist eine unbeschränkte Freiheit gelassen, sowohl hinsichtlich der Anzahl der verschiedenen Buchstaben in einer Gruppe, als auch hinsichtlich der Anzahl der Glieder einer Gruppe.

Digitized by Google

Abgesehen von dem Mangel, wie ihn die Methode Caesars hat, ist Bacons Methode ziemlich umständlich und unbequem, da man sich bei Anwendung derselben stets eines schriftlichen Schlüssels bedienen müsste, was überhaupt immer als ein Mangel einer Geheimschriftmethode anzusehen ist. —

Jenem Mangel — dem der Methode Caesars analog — liesse sich allerdings abhelfen, indem man mit der Anwendung den Gebrauch eines Wahlwortes verbindet.

Chiffriert man z. B. das Wort: „Gefahr“ nach obiger Methode, so ergibt sich mit Anwendung des Wahlwortes: „Leidenschaft“ folgendes:

g i i g i g g i i i g i i i i g i g i g g i i i g i i g i g
l e i d e n s c h a f t l e i d e n s c h a f t l e i d e n.

Hierauf wird jedem Gruppenbuchstaben der ihm entsprechende Buchstabe des Wahlwortes zur Seite gestellt, sodass sich das Chiffrewort — bei vorausgesetzter fünfgliedrigen Gruppierung — so gestaltet:

glieiigdiegngsicihiagfitilieiigdiegnisgcghiaifitglieiigdiegn.

So würden also je 10 Chiffrebuchstaben *1* Buchstaben der Klarschrift ausdrücken.

2. Einfacher als der vorige Vermehrungschiffre ist der nachfolgende, der in vielerlei Variationen zu „Geheimschrifträtseln“ verwendet wird. Der Grundgedanke dieses Vermehrungschriffres ist der, durch Einschalten von beliebigen Buchstaben zwischen diejenigen der Wörter der Klarschrift neue oder wortähnliche Sprachformen zu bilden; oder auch es werden gewisse Buchstaben aus den Wörtern der Klarschrift ausgestossen und durch Hinzufügen anderer Buchstaben neue Wortformen gebildet.

Ein Beispiel erster Art:

„Wir werden dich erwarten“. —

„ewahir weturadien adimech elirwefaritogen“.

Ein Beispiel zweiter Art:

„Der Schlüssel ist entdeckt“.

(nach Ausstossung der Vocale: dr schlssl st ntdckt):

„edar escahlissol sita notidickta“.

Besondere Vereinbarungen, z. B. welche Buchstaben jeweils einzuschalten sind, können dem Correspondenten das Dechiffrieren erleichtern. —

Digitized by Google

Die Anwendung dieser Methode ist wohl leicht durchzuführen und eignet sich auch für grössere Mitteilungen; um aber das Geheimnis zu sichern, müssen schon noch andere Sicherungsmomente in diese Methode eingeführt werden.

XIV.

Der Wort- und Silbenchiffre.

1. Wie in voriger Methode ein Buchstabe der Klarschrift durch mehrere nach Verabredung gesetzte Chiffrebuchstaben ausgedrückt wird, kann er auch durch ein beliebiges Wort ersetzt werden; z. B. *a* = Welt, *b* = Zeit, *c* = Osten, *d* = Vater etc. (Tritheims Wortchiffre). Aber auch diese Methode ist mangelhaft und sehr umständlich.

2. Weit besser ist dieser Wortschiffre: Man wähle sich irgend ein Wörterbuch (Lexikon), in welchem die Wörter auf gespaltenen Colonnen stehen; dabei setzt man nun für die Wörter der Klarschrift jeweils diejenigen Wörter, die jenen in dem betreffenden Wörterbuch gegenüber (oder unter ihnen) stehen. Für die Flexionen oder für kleine oft vorkommende Wörter verabredet man am besten besondere Zeichen. —

3. Hierher gehört auch der sog. Silbenchiffre. Dieser besteht darin, dass nur gewisse Silben eines Schriftstückes Geltung haben, z. B. die beiden ersten und letzten Zeilen eines Briefes sollen nicht gelten, in allen übrigen aber in jedem ersten und dritten Worte die 1., 2. oder letzte Silbe *).

Diese drei Methoden sind wegen ihrer umständlichen und mühsamen Anwendungsweise als praktische Chiffremethoden nicht zu empfehlen. —

XV.

Der Vokalchiffre.

Wir kommen nun zu einer weiteren interessanten Chiffremethode, bei der nur durch die fünf Vokale a, e, i, o, u chiffriert wird. Daher heisst sie auch Vokalchiffre. — Als Schlüssel dient ein kleines Quadrat von 25 Feldern, welches in der Sprachlinie wie in der Wahllinie (Siehe Methode VI) mit den einfachen Vokalen beschrieben ist, während die Felder des Quadrates mit den 25 Buchstaben des Alphabetes nach Belieben ausgefüllt werden. — In dieser Chiffremethode wird nun jeder Buchstabe der

*) Vgl. ausserdem Klübers Kryptographik S. 86 ff.

Digitized by Google

Mitteilung durch je zwei Vokale dargestellt, von denen der eine den Ausgangspunkt einer Horizontalreihe, der andere den Ausgangspunkt einer Vertikalreihe bildet (wie oben in Methode VI, Ziffer 3).

Nachstehend die Tabelle:

	a	e	i	o	u
a	v	s	w	a	z
e	b	e	o	n	r
i	d	l	c	x	u
o	q	y	h	m	p
u	t	i	f	k	g

Hiernach ist z. B. *a* = ao, *b* = ea, *c* = ii, *f* = ui, ... *z* = au. —

Das Wort „Grenze“ hiesse nach dieser Methode:

uueueeeoauee. —

Die Sprach- und Wahllinie kann auch durch Ziffern gebildet werden *).

Diese Geheimschriftmethode ist sehr einfach und leicht fasslich; da aber gleiche Buchstaben jeweils durch die gleichen Doppelvokale ausgedrückt werden müssen, so vermag sie nicht die gleiche Sicherheit zu bieten, wie andere Geheimschriften. — Aber durch Combination mit einer anderen Methode vermag sie wohl zur Undurchdringlichkeit des Geheimnisses manches beizutragen. —

Vgl. hierzu den Vermehrungschiffre, Methode XIII (dieses Abschnittes). —

XVI.

a) Geheimschrift eines Nihilisten.

Höchst interessant ist nachstehende Geheimschrift der Nihilisten. — Die Nihilisten bedienen sich zur Bezeichnung der einzelnen Felder des in kleine Quadrate eingeteilten Vierecks eines Wahlwortes, indem sie dessen einzelne Buchstaben nach ihrer Reihenfolge im gewöhnlichen Alphabet nummerieren und die so erhaltene Ordnungszahl sowohl in die Sprachlinie als auch in die Wahllinie (Siehe Methode VI) einzeichnen.

Nehmen wir z. B. das Wahlwort: Isolde, dessen einzelne Buchstaben nach der natürlichen Reihenfolge im Alphabet geordnet

1 2 3 4 5 6
d e i l o s ergeben,
folglich: 3 6 5 4 1 2
I s o l d e.

*) Vgl. Methode XVII, Fig. a.

Digitized by Google

Jetzt ist nur noch die erhaltene Ordnungszahl 3 6 5 4 1 2 von Bedeutung; in der Wahllinie gibt sie die Reihenfolge der Zeilen an, in der Sprachlinie diejenige der einzelnen Buchstaben*)

Wahllinie	Sprachlinie 3	6	5	4	1	2
3	r	n	e	g	m	o
6	v	z	i	n	s	k
5	g	s	u	r	e	n
4	s	h	c	u	b	e
1	h	r	e	w	i	c
2	d	h	c	i	d	e

Es soll nun die geheime Mitteilung:

rnegmo vzinsk gsuren
shcube hrewic dhcide

entziffert werden, wobei zugleich das Verfahren beim Chiffrieren erkennbar wird. Nachdem diese Mitteilung, die übrigens auch in mehr- oder weniger-stelligen Wörtern niedergeschrieben werden kann, auf nebenstehende Weise in die einzelnen Quadrate eingetragen ist, wird noch die Sprach- und Wahllinie eingezeichnet. Bei Ziffer *1* der Wahllinie, die uns die Reihenfolge der Zeilen angibt, ist nun zu beginnen; und da die Sprachlinie die Reihenfolge der Buchstaben (der Klarschrift) kennzeichnet, so muss an der Stelle, wo die Vertikalreihe der Ziffer *1* die Horizontalreihe der Ziffer *1* trifft, der erste Buchstabe der Mitteilung stehen, (also *i*); die nächsten fünf Buchstaben der zu dechiffrierenden Mitteilung enthält noch alle die Horizontalreihe der Ziffer *1*, ihre richtige Ordnung geben die Ziffern der Sprachlinie an: wo demnach die Vertikalreihe der Ziffer *2* die Horizontalreihe der Ziffer *1* trifft, da steht der zweite Buchstabe der Mitteilung (c), und wo die Vertikalreihe der Ziffer *3* (4, 5, 6) die Horizontalreihe der Ziffer *1* trifft, da steht der *3.* (4. 5. 6.) Buchstabe h, (w, e, r).

Auf gleiche Weise werden der Reihe nach die Buchstaben der 2. 3. 4. 5. 6. Horizontalreihe aufgesucht, bezw. geordnet, sodass man schliesslich die Mitteilung erhält:

„Ich werde dich morgen besuchen. Gruss".

Die übrigbleibenden Buchstaben k v n i z sind bedeutungslos und sollen nur die leerbleibenden Felder ausfüllen. —

Je grösser die Mitteilung sein soll, desto mehr Felder müssen zur Verfügung stehen, weshalb man auch ein grösseres Wahlwort (oder kurzes Citat) aussuchen muss; dabei wird man aber

*) Vgl. oben Methode VIII.

Digitized by Google

vermeiden müssen, dass in dem Wahlwort ein Buchstabe nicht zweimal vorkommt, event. müsste der sich wiederholende Buchstabe fortfallen.

Nach den erwähnten Angaben wird es nun nicht mehr schwer sein, die Buchstaben der zu chiffrierenden Mitteilung in die Felder einzutragen, nachdem die Felder nebst der Sprach- und Wahllinie gebildet sind.

Der Schlüssel besteht bei dieser Geheimschrift in einem Wahlwort und in der angegebenen Art der Nummerierung. Von dieser Seite aus wird (bei gehöriger Vorsicht der Anwendung) eine Entzifferung unmöglich sein. Aber auch im Allgemeinen ist diese Methode zuverlässig und eignet sich zu kurzen geheimen Nachrichten vorzüglich *). —

XVII.

b) Geheimschrift eines Nihilisten.

Die Nihilisten bedienen sich zur geheimen Verständigung auch eines Zahlenchiffres, der einen schlagenden Beweis für den Erfindungsgeist dieser Elemente bietet. — Die Grundlage desselben bildet die Idee, dass durch irgend eine Rechenweise ein Buchstabe umschrieben werden kann z. B. 11 + 14 = 25 = k, 25 — 14 = 11 = b. Diese Idee wird nun mit dem Grundgedanken der Methode XV. in Verbindung gebracht, wobei nur statt der Vokale Ziffern gesetzt werden.**)

Nach Fig. a ist z. B. d = 14 oder 2 + 12 = d
u = 45 „ 39 + 6 = u
r = 42 „ 12 + 30 = r
c = 13 „ 9 + 4 = c
h = 23 „ 18 + 5 = h

Fig. a.

(Zehner) \ (Einer)	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

Um nun diese Addition in Anwendung zu bringen, bezeichnet man jeweils die beiden Summanden mit Buchstaben, von denen der eine einen Buchstaben der zu chiffrierenden Mitteilung, der andere aber einen Buchstaben eines Wahlwortes darstellt. Die Summe d. h. die beiden addierten Summanden ergeben das eigentliche Chiffrezeichen. Um nun wieder den Buchstaben der Klarschrift zu erhalten, muss man von der Chiffrezahl

*) Vgl. hierzu III. Abschnitt, I. Capitel dieser Darstellung.
**) Vgl. Methode XVIII, Fig. c.

Digitized by Google

(d. i. der Summe) denjenigen Summanden subtrahieren, der den Buchstaben des Wahlwortes darstellt.

Ein Beispiel wird es klar machen.

Fig. b.

I.	E	s	d	r	o	h	t	G	e	f	a	h	r	r	e	i	s	e	a	b				
II.	15	43	14	42	34	23	44	22	15	21	11	23	42	42	15	24	43	15	11	12				
III.	P	o	l	i	z	e	i	P	o	l	i	z	e	i	P	o	l	i	z	e				
IV.	35	34	31	24	55	15	24	35	34	31	24	55	15	24	35	34	31	24	55	15				
V.	50	77	45	66	89	38	68	57	49	52	35	78	57	66	50	58	74	39	66	27				

Linie I. stellt die Mitteilung dar, Linie II. die Chiffrierung derselben nach der erwähnten Weise (Fig. a.), Linie III. enhält das Wahlwort, Linie IV. dessen Ciffrierung nach Fig. a., Linie V. die Addition von Linie II. und IV.

Um nun die geheime Depesche:

Fig. c.

50	77	45	66	89	38	
68	57	49	52	35	78	57
66	50	58	74	39	66	27

zu entziffern, schlägt man folgenden Weg ein:

Fig. d.

V.	50	77	45	66	89	38	68	57	49	52	35	78	57	66	50	58	74	39	66	27				
III.	P	o	l	i	z	e	i	P	o	l	i	z	e	i	P	o	l	i	z	e				
IV.	35	34	31	24	55	15	24	35	34	31	24	55	15	24	35	34	31	24	55	15				
II.	15	43	14	42	34	23	44	22	15	21	11	23	42	42	15	24	43	15	11	12				
I.	E	s	d	r	o	h	t	G	e	f	a	h	r	r	e	i	s	e	a	b				

Hierbei wird nun Linie IV. von Linie V. subtrahiert, die Differenz (Linie II.) wird nach Fig. a. reduziert in die Klarschrift.

Ganz gleich ist das Verfahren, wenn man in Fig. b. Linie II. und IV. zahlenweise mit einander multipliziert, wobei dann bei Fig. d. die Zahlen der Linie V. dividiert werden müssen durch die unter ihnen stehenden Zahlen der Linie IV. Das Resultat in Linie II. (Fig. d.) wird immer gleich bleiben. —

So einfach diese Chiffremethode ist, so sinnreich ist sie auch; sie vermag auch volle Sicherheit des Geheimnisses zu gewähren. —

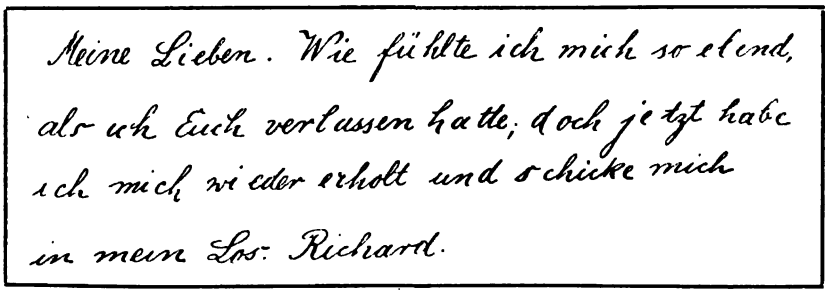
Digitized by Google

XVIII.

c) Geheimschrift eines Nihilisten.

An Einfachheit und Genialität übertrifft unstreitbar die jetzt zu besprechende Geheimschrift die beiden vorhergegangenen Methoden. Der russische politische Gefangene weiss selbst den wachsamsten Beamten des russischen Geheimschriftenbureaus, durch dessen Hände die Briefe an seine Angehörigen gehen, zu täuschen, dies lässt die nachfolgende Chiffremethode klar erkennen.

Fig. a.



Diese harmlosen Zeilen verbergen nun eine geheime Mitteilung.

Die Thatsache, dass man beim Schreiben oft unwillkürliche Unterbrechungen innerhalb eines Wortes eintreten lässt, hat der schlaue Gefangene zur Verdeckung seines Geheimnisses benutzt. Dabei hat er danach gestrebt, bei seiner allgemeinen Mitteilung in unauffälliger Weise Gruppen von Buchstaben zu bilden, die jeweils irgend eine zweistellige Zahl ergeben, die nach einer schon bekannten Methode in die Klarschrift reduziert werden.

Um nun anzudeuten, dass der erste Buchstabe des nächstfolgenden Wortes noch zur vorhergehenden Gruppe gehört, wird der Endstrich des letzten Buchstabens jeweils nach rechts ausgezogen, während eine Abrundung nach oben stets das Ende einer Gruppe bedeutet. —

Nach meiner Ansicht ist es aber noch weniger auffallend, wenn das Vorhandensein eines Aufstriches am folgenden Worte die Verbindung mit dem vorhergehenden Worte — zum obigem Zwecke — andeuten soll, das Fehlen desselben aber die Trennung der beiden Wörter. Bei Majuskeln und Minuskeln wie m, n, r etc. ist dies durch geraden bezw. nach einwärts gebogenen Aufstrich ersichtlich zu machen.

In der folgenden Figur werden dann die geheimen Gruppen der Originalmitteilung ihren beabsichtigten Unterbrechungen ent-

Digitized by Google

sprechend nebeneinander und über jede Gruppe die Zahl der sie bildenden Buchstaben geschrieben.

Fig. b.

5	1 : 1	5	: 4	2 : 3	3 : 2	4 : 1	3 : 2	3						
Meine	L i	ebenw	iefü	hl	tei	chm	ic	hsoe	l	end	al	sic		
4	4 : 1	5 : 1	1 : 3	1 : 3	1 : 1	5 : 1	2 : 4	2						
heuc	hver l	assen	h a	tte	d	och	j e	tztha	b	ei	chmi	ch		
2	4 : 1	5 : 2	1 : 1	5										
wi	eder e	rholt	un	d	s	chick	emichinmeinlosrichard.							

Je 2 nebeneinander stehende Ziffern bilden eine Zahl, die jetzt nach Fig. c. dechiffriert wird (vergl. Methode XVII. Fig. a.)

Fig. c.*)

(Zehner) \ (Einer)	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

Fig. d.

51 = v	31 = l
15 = e	31 = l
42 = r	15 = e
33 = n	12 = b
24 = i	42 = r
13 = c	24 = i
23 = h	15 = e
44 = t	21 = f
15 = e	15 = e
11 = a	

Resultat: „Vernichte alle Briefe.“

Vergleiche hierzu: III. Abschnitt, IV. Capitel dieser Darstellung.

XIX.

Chiffriermethode mit Anwendung mehrerer Alphabete.

Die jetzt folgende Methode der Geheimschrift sucht den Mangel von Julius Caesar's Geheimschrift (sh. Methode I) dadurch zu beseitigen, dass sie im Princip für jedes Wort der zu chiffrierenden Mitteilung ein neues Alphabet verwendet. Dies geschieht nun so:

*) Sog. „Schachbrettchiffre“, der sich als Versetzungsmethode sehr gut eignet.

Digitized by Google

	I	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
5	T	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	k
6	U	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
3	G	i	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
2	E	w	x	y	z	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	v
4	N	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	k	l	m	n
1	D	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r
	I	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Das Wahlwort heisst hier: Tugend, dessen Buchstaben je ein neues Alphabet bezeichnen sollen.

Die Mitteilung: „Komme heute nicht“ — ist nun folgendermassen zu chiffrieren: Man geht von der mit I. bezeichneten Alphabetreihe aus, in der zunächst der zu chiffrierende Buchstabe aufzusuchen ist, und findet im Kreuzungspunkt der Vertikalreihe und der entsprechend anzuwendenden Horizontalreihe den Chiffrebuchstaben. Für die Buchstaben des ersten Wortes (komme) sind sodann die entsprechenden Buchstaben der T-Linie einzusetzen, also: uywwp; für die Buchstaben des zweiten Wortes (heute) die der U-Linie, also: lhxwh, für die Buchstaben des dritten Wortes (nicht) die der G-Linie, also: vrlqb.

Wäre die Mitteilung grösser, so würden die Buchstaben des vierten Wortes nach dem Alphabet der E-Linie versetzt und die des 7. Wortes wieder nach dem der T-Linie u. s. w.

Hiermit ist allerdings der Mangel von Caesars Methode nicht vollständig beseitigt, denn die zwei *w* im Worte uywwp lassen auf eine Verschärfung (oder Dehnung) schliessen, die beiden *h* im Worte lhxwh bezeichnen ebenfalls einen gleichen Buchstaben; ausserdem ist stets die Anzahl der Buchstaben eines Wortes angedeutet, was alles für eine unbefugte Entzifferung von Vorteil sein kann. — Darum halte ich es entschieden für besser, bei jeder Silbe das nächstfolgende Alphabet zu verwenden, dann ergibt sich:

T U G E N
kom me heu te nicht.
uyw ph qnc pa awqvg.

Man wird jetzt gleich einsehen, dass durch diese Trennung gleiche Buchstaben des Wortes stets durch verschiedene Buchstaben ausgedrückt werden können.

Digitized by Google

An Stelle des Wahlwortes, dessen Wert mir bei dem bisherigen Verfahren noch nicht als begründet erscheint, könnte man mit dem gleichen Erfolg die Ziffern *1* bis *6* untereinander schreiben.

Man kann ihm aber doch einen gewissen Wert beilegen, wenn man (wie in Methode XVI) die einzelnen Buchstaben desselben nach der natürlichen Reihenfolge im Alphabet nummeriert. (Sh. die Fig.) So ist nun die Wahl der untereinanderstehenden Alphabete genau vorgeschrieben, in dem das erste Wort (bezw. dessen erste Silbe) der Mitteilung durch die Buchstaben der D-Linie, das zweite Wort (bezw. die 2. Silbe des 1. Wortes) durch die Buchstaben der E-Linie etc. chiffriert wird.

Hiernach lautet obige Mitteilung z. B. nach Silben getrennt:

1	2	3	4	5
D	E	G	N	T
kom	me	heu	te	nicht.
bfd	ha	qnc	gs	xtnsd.

Dechiffrierung:

D	E	G	N	T
bfd	ha	qnc	gs	xtnsd.
kom	me	heu	te	nicht.

Der Wert dieses Verfahrens liegt wohl darin, dass der schriftliche Schlüssel d. h. die beliebige (aber verabredete) Gruppierung der Alphabete nie zum Verräter des Geheimnisses werden kann, insoferne nicht das Wahlwort dazu geschrieben ist, was absolut nicht notwendig ist; denn das Wahlwort mit seiner Verwertung behält man als eigentlichen Geheimnisschlüssel im Gedächtnis und bringt es bei jeder Dechiffrierung erforderlichenfalls an der schriftlichen Alphabetentabelle an. Mit den erwähnten Ergänzungen gestaltet sich vorliegende Methode zu einer ganz praktischen und zugleich sicheren Geheimschrift; praktisch, weil sie auch die Chiffrierung grösserer Mitteilungen zulässt. (Vergleiche Methode VII, Ende.)

Während bei den bis jetzt besprochenen Geheimschriftmethoden im wesentlichen nur mit Hilfe der Buchstaben chiffriert wurde, werden bei den nachfolgenden Methoden ausschliesslich Ziffern bezw. Zahlen als Chiffrezeichen angewendet.

Abgesehen davon, dass bei den meisten obigen Methoden statt Buchstaben auch Ziffern bezw. Zahlen bequem einzuführen

Digitized by Google

sind, gibt es einige besondere Zahlenchiffres, deren Besprechung hier folgen soll.

XX.

Kircher's abacus numeralis.

	a	b	c·····	w	x	z
a	1	2	3·····	22	23	24
b	2	3	4·····	23	24	1
c	3	4	5·····	24	1	2
⋮	⋮	⋮	⋮	⋮	⋮	⋮
w	22	23	24·····	19	20	21
x	23	24	1·····	20	21	22
z	24	1	2·····	21	22	23

Den Tritheimischen Multiplicationschiffre (Sh. Methode VI) hat Kircher derart in einen Zahlenchiffre umgewandelt, dass er die Buchstaben von *a*—*z* jeweils durch Zahlen von 1—24 ersetzte, ohne jedoch Wahl- und Sprachlinie zu verändern. (Kirchers „abacus numeralis"). Das Chiffrieren und Dechiffrieren ist wie beim Multiplicationschiffre vorzunehmen. (Vgl. diesen.)

XXI.

Ein Zahlenchiffre nach Caesar's Methode.

Sehr einfach wäre auch ein Zahlenchiffre nach Caesars Methode herzustellen; allerdings müssten dann durch Einschalten von anderen Zahlen (von 25—99), die teils Interpunktionen, teils Zahlen, Nieten etc. bezeichnen sollen, die vorhandenen Mängel beseitigt werden.

Man kann weiterhin durch Zahlen nicht bloss einzelne Buchstaben ausdrücken, sondern auch Silben, Wörter, sogar ganze Phrasen. Zu diesem Zwecke werden besondere Chiffrier- bezw. Dechiffriertabellen aufgestellt, von denen in Klübers Kryptographik und in Fleissners Handbuch der Kryptographie ein Beispiel zu finden ist.

XXII.

Mirabeau's Methode.

Ein sehr brauchbarer Zahlenchiffre ist Mirabeau's Methode: Hiernach werden die 25 Buchstaben des Alphabetes in fünf Gruppen von je fünf Gliedern eingeteilt,

Digitized by Google

	1.					2.					3.					4.				
also z. B.	s	v	a	c	y	e	x	f	l	n	o	h	z	w	b	d	u	m	i	q
	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5

	5.				
	g	p	k	r	t
	1	2	3	4	5

Nach dieser Einteilung kann man jeden Buchstaben durch eine zweistellige Zahl ausdrücken, wobei deren Zehner die Gruppe, ihr Einer aber die betreffende Stelle des Buchstabens in der Gruppe angibt, z. B. $n = 25$, $k = 53$, $a = 13$ etc.

Die Ziffern 6, 7, 8, 9, 0 sind beliebig als Nieten zu verwenden.

Diese Methode lässt aber noch eine praktische Variation zu, da man die einzelnen Zahlenwerte auch in Form eines Rechenexempels aneinanderreihen kann, z. B. in Bruch- (oder Dezimal-)form, wobei im Zähler des Bruches die Ziffer der Gruppe, im Nenner die Ziffer des betreffenden Buchstabens verborgen wird. —

So könnte man beispielsweise die Mitteilung: „Schreibe sofort“ chiffrieren:

$$\frac{701}{18}+\frac{1006}{470}+\frac{36}{20}-\frac{759}{848}+\frac{726}{106}-\frac{940}{409}+\frac{8039}{7500}+\frac{802}{718}$$

$$+\frac{910}{717}+\frac{73}{189}+\frac{20}{39}-\frac{377}{1807}+\frac{568}{460}+\frac{57}{589}$$

oder: 701,18 (= 1,1) $\times$ 1006,47 (= 1,4) $\times$ 36,2 (= 3,2)

$$\times\ \frac{5}{48}\ \times\ 2{,}106\ \times\ \frac{94}{409}\ \text{etc.}$$

Digitized by Google

	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	1	2	3	4	5	6	7	8	9	0	,	.
I.	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52
II.	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56
III.	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63

XXIII.

Ein Zahlenchiffre mit wechselndem Alphabet.

Wenn man einen schriftlichen Schlüssel mit gehöriger Vorsicht anzuwenden weiss, so kann man nachstehenden Zahlenchiffre mit Nutzen anwenden. —

Wechselzeichen:

Die I. Zahlenreihe wird durch eine der drei folgenden Zahlen angedeutet: 11 15 63 Die II. Z.-R.: 12 68 64

Die III. Z.-R.: 13 67 65

Nieten:

14, 66, 69—99.

Dieser Zahlenchiffre lässt eine grosse Anzahl Variationen zu; der erste Vorteil muss aber immer der bleiben, dass man für den einzelnen Buchstaben mehrere Zahlenreihen anwenden kann, wobei der Wechsel einer solchen Reihe durch ein entsprechendes Wechselzeichen angekündigt wird.

Die Mitteilung: „Es droht Verrat“ lässt sich z. B. so chiffrieren:

13 31 44 30 43 40 34 64 38 40 24 36 15 32 16 34 51.

Mit der dritten Zahlenreihe wurde begonnen, was die Zahl *13* andeutet, bei *t* (im Worte droht) wurde die zweite Zahlenreihe angewendet, was die Zahl *64* andeutet, bei dem zweiten *r* (im Worte Verrat) wurde die erste Zahlenreihe benützt, was die Zahl *15* angibt. Es wird also ein Wechsel am besten da stattfinden können, wo (besonders in einem Worte) der gleiche Buchstabe sich wiederholt. — Ausserdem sind noch an beliebigen Stellen Nieten einzuhalten, sodass die so chiffrierte Mitteilung schon ziemlich zuverlässig sein kann. —

Bei der Dechiffrierung werden zunächst die Nieten durchgestrichen und dann die einzelnen Zahlen der jeweils angedeuteten Zahlenreihe durch die entsprechenden Buchstaben ersetzt.

Digitized by Google

XXIV.

Ein Zahlenchiffre mit Rechenoperationen.

Durch Rechenoperationen lassen sich auch zahlreiche praktische Zahlenchiffres zusammenstellen; so durch Addition bezw. Subtraction, durch Multiplikation bezw. Division. Auf diesem Wege lassen sich sehr bequem die einzelnen gleichen Buchstaben verschieden ausdrücken. Es sei z. B. folgender Zahlenchiffre anzuwenden, wobei also die einzelnen Zahlen jeweils durch Summen bezw. Produkte auszudrücken sind.

a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	v	w	x	z
4	1	3	5	7	9	11	13	15	2	6	8	10	12	14	16	18	17	19	21	23	20	22	24

Nach diesem Chiffreschlüssel wird das Wort „Geheimnis“ ausgedrückt:

11 7 13 7 15 8 10 15 17

Nun werden die einzelnen Zahlen in ihrer Grösse vermehrt durch Addition bezw. Multiplikation, wobei hinter die Summe bezw. hinter das Produkt der Summand bezw. der Multiplikator — je nach Verabredung — geschrieben wird, sodass der Empfänger der Mitteilung sofort erkennt, um wieviel die Zahl zu verringern ist, um ihre ursprüngliche Grösse zu erhalten. Z. B. $11 + 4 = 15$, also Chiffrezeichen: 154; die Ziffer 4 zeigt an, dass 15 um 4 zu verringern sei, um die ursprüngliche Zahl (11) zu erhalten.

Obiges Wort könnte beispielsweise chiffriert so aussehen:

154 92 207 114 216 102 177 161 214

Analog sind die ursprünglichen Zahlen durch Multiplikation zu verändern. Z. B. $11 \times 5 = 55$, als Chiffrezeichen: 555; die Ziffer 5 am Ende zeigt an, dass 55 durch 5 zu dividieren sei, um die ursprüngliche Zahl (11) zu erhalten.

Hiernach obiges Beispiel:

555 213 262 497 302 729 303 453 342

Die Anwendung beider Rechenexempel in einer Mitteilung kann man durch besonders verabredete Zahlen, die z. B. nur durch sich selbst teilbar sind wie 13, 17, 23, 53 etc. anzeigen; solche Zahlen lassen sich natürlich auch mit Vorteil als Nieten verwenden, sodass ein geschickter Gebrauch dieser Art von Zahlenchiffre ziemliche Sicherheit des Geheimnisses gewähren kann, zumal ein schriftlicher Schlüssel bald entbehrlich wird. —

Am besten bezeichne ich diesen Chiffre: „Arithmetischer Vermehrungschiffre.“

Digitized by Google

Wird man die Reihenfolge der nach diesem Chiffre gebildeten Zahlen noch mit einer Versetzungsmethode umgestalten, so kann man die geheime Mitteilung geradezu undechiffrierbar machen.*)

Ein Versetzungschiffre, der sich hier besonders gut eignet, ist folgender:

Die obige geheime Mitteilung:

1	2	3	4	5	6	7	8	9
154	92	207	114	216	102	177	161	214

lässt sich hinsichtlich der Reihenfolge der einzelnen Zahlen nach der Versetzungsordnung: 3, 6, 9 etc.; 2, 5, 8, 11 etc.; 1, 4, 7, 10 etc. verändern:

3	6	9	2	5	8	1	4	7
207	102	214	92	216	161	154	114	177

Oder es können gewisse Ziffern in einer Zahl noch nachträglich vertauscht werden, z. B. die beiden letzten: statt 154 nämlich 145, also:

145 29 270 141 261 120 177 116 241

XXV.

Der Massstabchiffre.

Eine ganz einfache aber sehr zu empfehlende Geheimschriftmethode ist der Massstabchiffre, bei dem die Buchstaben des Alphabetes in Felder von gleicher oder — besser — von verschiedener Grösse in gerader, fortlaufender Linie eingetragen werden.

Es ist z. B. ein Papierstreifen so eingeteilt:

1 ctm	2	3	4	5	6	7	8	9	10 ctm
h	l	e	t	f	s	n	i	r	v

24 ctm	23	22	21	20	19	18	17	16	15 ctm

Die Buchstaben der geheimen Wörter werden nun so chiffriert, dass man für den ersten Buchstaben die Entfernung von einem Endpunkt des Massstabes bis zu dem betreffenden Buchstaben selbst setzt. Z. B. n = 7 (ctm); bei jedem weiteren Buchstaben wird von dem Endpunkt der letzten Entfernung ausgegangen, um weiter zu messen, also r = 2 (ctm.)

*) Auch die Chiffremethode nach Methode XVIII. Fig. c. kann hier Verwendung finden.

Digitized by Google

Hierbei wird es oft vorkommen, dass man von rechts nach links die Entfernung eines Buchstabens von einem anderen abzumessen hat; für diese Fälle sind besondere Punktierzeichen zu verabreden, um diese Zahlen von jenen (von links nach rechts gemessenen) Zahlen zu unterscheiden.

Das Wort „Freiheit" könnte man nun so chiffrieren:

(20 oder) 5 4 6 5 7 2 5 4

Diese Chiffriermethode lässt auch eine Anzahl Variationen zu, sodass man nicht streng an obiges Beispiel gebunden ist.

Vgl. hierzu auch den Massstabchiffre im zweiten Abschnitt dieses Werkchens Capitel IV., sub 3.

Hier will ich auch ein Beispiel angeben, bei dem die Felder des Massstabes ungleich gross gewählt sind, welche Variation wohl sehr vorteilhaft sein dürfte.

1½ ctm	3½	4½	6	7½	9½	11	12½ ctm	
m	c	e	r	i	a	z	h	↣
1½ ctm	2	1	1½	1½	2	1½	1½ ctm	

Die Abmessung der einzelnen Entfernungen kann nun wie im vorigen Beispiel vorgenommen werden, oder man kann bei jedem Buchstaben die Messung von dem einen Endpunkte des Massstabes aus vornehmen, wobei dann jede Punktierung überflüssig wird.

Nach der ersten Art liesse sich das Wort „Rache" so chiffrieren:

6 3½ 6 9 7½

Nach der zweiten Art:

6. 9½ 3½ 12½ 4½
oder: 5½ 9¼ 3⅓ 12⅕ 4³/₁₀
oder: 5,2 9,3 3,5 12,4 4,3 etc.

Der Grundgedanke der beiden letzten Chiffrierarten ist der, dass man für irgend ein Mass z. B. für 1½ alle diejenigen Bruchzahlen benützen kann, welche dieses Mass nicht unter- oder übersteigen. So ist also die Möglichkeit gegeben, für gleiche Buchstaben jeweils verschiedene Zahlenausdrücke zu setzen, was ja ein Haupterforderniss einer Sicherheit bietenden Geheimschrift ist.

Am Schlusse dieses ersten Abschnittes möchte ich noch einige praktische Punktiermethoden besprechen.

Digitized by Google

Der massgebende Gedanke einer Punktiermethode ist der, die Chiffrebuchstaben in einem offenkundigen Schriftstück oder einer Zeitung durch unscheinbare Erkennungsmerkmale (Punktierzeichen) wie Punkte, Striche oder Nadelstiche, in der Nähe des betreffenden Buchstabens angebracht, dem Empfänger der geheimen Mitteilung anzudeuten. Hierher gehört vor allem Schotti's Punktiermethode, die unten folgt.

Aber auch Wörter und Zahlen, die in den Zusammenhang eines Schriftstückes unauffällig eingeflochten werden, können die Eigenschaft eines Punktierzeichens in sich tragen. Hierher gehört in erster Linie Heidels Punktiermethode (Methode XXVII.), sowie meine im dritten Abschnitt (Capitel VI.) angegebenen Punktiermethode.

In zweiter Linie ist auch der sog. Buchchiffre (Methode XXVIII.) hier zu erwähnen.

Ueber andere Punktiermethoden vergl. den zweiten Abschnitt dieses Werkes (Cap. IV.) und den dritten Abschnitt (Cap. V.)

XXVI.

Schotti's Punktier-Methode.

Zur Anwendung dieser Methode bildet man sich ein Zahlenalphabet bei Vermeidung der arithmetischen Reihenfolge der Zahlen. Z. B.

a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r
14	12	3	16	10	23	13	9	2	7	21	11	20	24	4	6	19

s	t	u	v	w	x	z
15	22	8	17	1	5	18

Soll nun beispielsweise das geheime Wort „Flucht" in einem gleichgiltigen Schriftstück (oder einer Zeitung) einpunktiert werden, so ist folgendermassen zu verfahren:

Der Buchstabe *f* ist durch die Zahl *23* ersetzt, also muss am *23.* Buchstaben — vom Anfang des Schriftstückes an gezählt — das verabredete Punktierzeichen angebracht werden.

Der Buchstabe *l* ist durch die Zahl *21* ersetzt, also muss — vom ersten punktierten Buchstaben aus gezählt — der *21.* Buchstabe des Schriftstückes das Punktierzeichen erhalten; bei *u* hat dann der *8.* Buchstabe — von dem zuletzt punktierten Buchstaben aus gezählt — das Punktierzeichen zu erhalten u. s. f.

Digitized by Google

Es ist also jeweils vom letzten Punktierzeichen aus der nächste Buchstabe zu suchen (bezw. abzuzählen) und zu punktieren. —

Man erkennt nun aber sogleich, dass bei einer grösseren Mitteilung, sowie durch die teilweise hohe Zahlenbezeichnung der Buchstaben auch ein grosses Schriftstück zur Einpunktierung erforderlich wird. Diesem Misstand lässt sich aber durch ein viel einfacheres Verfahren abhelfen. Ich chiffriere die geheime Mitteilung durch irgend eine bekannte Chiffremethode; sodann punktiere ich die einzelnen Chiffrebuchstaben in das Schriftstück oder in die Zeitung ein, sobald ich hier einen dem Chiffrebuchstaben gleichen Buchstaben antreffe. Hierbei kann man noch, um die Sicherheit zu steigern, das Punktierzeichen nicht an dem betreffenden Buchstaben selbst anbringen, sondern an irgend einer andern verabredeten Stelle, z. B. am 1., 2., 3. etc. Buchstaben links oder rechts von dem eigentlich zu punktierenden Chiffrebuchstaben. —

Bei dieser Gelegenheit will ich noch darauf hinweisen, dass die Correspondenz mit Anwendung dieser Punktier-Methode in pecuniärer Hinsicht die billigste ist, die überhaupt existiert; denn das Porto für Versendung von Drucksachen (Zeitungen), welche zur Einpunktierung der Chiffrebuchstaben benützt werden, ist durchwegs geringer als das Porto für Schriftstücke. —

In der Regel wird auch die Existenz einer geheimen Mitteilung verborgen bleiben, soferne nicht die Punktierzeichen zu auffallend angebracht sind.

Vgl. ausserdem den III. Abschnitt. Capitel V.

XXVII.

Heidel's Punktier-Methode.

Diese Methode beruht darauf, dass die im Zusammenhang eines Schriftstückes eingefügten geheimen Wörter durch irgend welche Zeichen in einem zweiten Absatze (Postscriptum) in der Weise angedeutet werden, dass an der gleichen Stelle, wie im ersten Absatze das geheime Wort, auch im zweiten Absatz ein Punktier-Wort steht, das durch seinen jeweiligen gleichen Anfangsbuchstaben erkennbar gemacht wird. Wenn also im ersten Abschnitt (des Schriftstückes) das 3., 7., 9., 14. etc. Wort ein geheimes ist, so

Digitized by Google

muss dies im zweiten Absatz gleichfalls durch das 3., 7., 9., 14. etc. Wort, das z. B. stets mit dem Buchstaben *e* beginnt, dem Empfänger der geheimen Mitteilung angedeutet werden. —

Ueber die Mängel dieser Methode vergleiche den dritten Abschnitt, Capitel II.

XXVIII.

Der Buchchiffre.

Das Wesen dieser Punktier-Methode besteht darin, dass durch Zahlen und Punkte auf gewisse Wörter, Silben und Buchstaben hingewiesen wird, die in einer Zeitung, einem Buche oder Lexikon enthalten sind und die Chiffrezeichen einer geheimen Mitteilung darstellen sollen.

Bei Anwendung dieser Methode müssen die beiden Correspondenten je das gleiche Exemplar des Buches besitzen. Am besten werden sich wohl Wörterbücher dazu eignen, da in solchen die nötigen Wörter eher und bequemer aufzufinden sind.

Das Verfahren ist nun dieses: Um ein bestimmtes Wort, eine bestimmte Silbe, einen bestimmten Buchstaben dem Correspondenten anzudeuten, bezeichnet der Schreiber der Mitteilung durch Zahlen die betreffende Seite (des Buches), die betreffende Zeile (nach Verabredung von oben oder von unten) und ebenso das betreffende Wort in der Zeile (von links oder rechts aus gezählt); soll in einem so angegebenen Worte noch die Silbe oder der Buchstabe angedeutet werden, so kann dies ebenfalls durch Zahlen geschehen oder durch eine entsprechende Anzahl von Punkten. —

Z. B. 106, 17, 4 oder:

106
17
4 } kann bedeuten:

Seite 106 (des gewählten Buches), Zeile 17 (von oben), 4. Wort (von links ausgezählt).

19 . . . kann bedeuten: 19. Wort, 3. Buchstabe.

26 . . . . kann bedeuten: 26. Wort, 3., 4. und 5. Buchstabe.

15 : · · : · : kann bedeuten: 15. Wort, 1., 4. und 6. Buchstabe.

Digitized by Google

$\overset{21}{\ldots}$ oder $\frac{3}{21}$ kann bedeuten: 21. Wort, 3. Silbe.

76, 8, $\overset{5}{\cdot}$ . . kann bedeuten:

Seite 76, Zeile 8, 5. Wort, 1. Silbe, 2. Buchstabe.

Diese Punktier-Methode ist allerdings etwas umständlich, solange aber das angewendete Buch als Geheimnis bewahrt bleibt, solange ist auch nicht an eine Entzifferung der geheimen Mitteilung zu denken. —

In neuester Zeit werden in vielen Staaten im diplomatischen Verkehr telegraphische Chiffriersysteme verwendet, deren Grundlage eigens zu diesem Zwecke eingerichtete Wörterbücher — aus verschiedenen Abtheilungen bestehend — bilden. —

(Näheres darüber ist in Fleissners Handbuch der Kryptographie S. 42 ff. zu finden). —

Bei Besprechung vorstehender Geheimschriftmethoden habe ich jeweils auf ihren Wert zur Verwendung als Chiffriermethoden hingewiesen und durch Angabe aller möglichen Variationen die Auswahl derselben dem Leser ziemlich mannigfaltig zu gestalten versucht. Es sei hier nur noch erwähnt, dass sich im allgemeinen die Zahlenchiffriermethoden zur privaten Anwendung am besten eignen. Uebrigens hat man auch in diplomatischen Kreisen eine besondere Vorliebe zu Zahlenchiffres. —

Geeignete Methoden, das Geheimnis (d. i. die geheime Mitteilung) in ostensiblen d. h. für jeden lesbaren Schriftstücken zu verbergen, findet der Leser im dritten Abschnitt (Cap. V und VI) dieser Darstellung. —

Digitized by Google

Zweiter Abschnitt.

Geheimschriftmethoden mit Hilfe anderer Zeichen.

Während die Geheimschriftmethoden des ersten Abschnittes nur ein Chiffrieren mit Buchstaben und Ziffern kennt, gibt es noch eine Reihe von Methoden, die auch andere Zeichen beim Chiffrieren in Anwendung bringen, und zwar Zeichen, die entweder im Schriftgebrauch bekannt sind, z. B. Buchstaben fremder Sprachen und anderer Schreibsysteme (z. B. Stenographie), Interpunktionszeichen, Musiknoten, mathematische und astronomische Zeichen und dgl., oder die von den beiden Correspondenten ganz willkürlich gebildet sind.

In weiterer Linie gehört auch die Anwendung sympathetischer Tinten (unten Methode VI.) hierher, die als Grundlage einer „Geheimschrift" die Unsichtbarkeit geschriebener Zeichen bezwecken.

Was das Verbergen der Existenz einer geheimen Mitteilung anlangt, so gehört im weiteren Sinn auch Schotti's Punktier-Methode (I. Abschnitt, Methode XXVI) hierher, sowie die hier zu besprechenden Punktier- und Linienchiffres.

Im engeren Sinne aber zählen hierher die Geheimschriften, mit sympathetischer Tinte geschrieben, und die im dritten Abschnitt zu besprechenden graphologischen Geheimschriftmethoden.

Das Bestreben, die geheime Mitteilung zu verdecken, um bei dritten Personen keinen Verdacht zu erregen, ist schon sehr alt. Von Hasdrubal, dem Heerführer der Karthaginienser, berichtet man, dass er die in eine Holztafel eingeschnittenen Zeichen durch eine Wachsschicht überzog und sie so dem Correspondenten überbringen liess. — Auch ist aus der Geschichte bekannt, dass man auf das geschorene Haupt eines Sklaven die geheime Mitteilung aufzeichnete und diesen dem Correspondenten zuschickte, nachdem

Digitized by Google

die geheime Mitteilung durch den Haarwuchs wieder verdeckt war. Zu erwähnen ist an dieser Stelle auch noch die geheime Polizeischrift des Grafen von Vergennes*), des Ministers der auswärtigen Angelegenheiten unter Louis XVI. Die Legitimationskarte eines Auswanderers barg nämlich gewisse Zeichen in sich, die die Polizei genau über die Persönlichkeit des angekommenen Fremden informierten: über Heimat, Alter, Stand, Religion; Gestalt; Temperament, Charakter; Tugenden, Laster; über seine wissentschaftliche Bildung; über seine Talente und Kenntnisse; ob verheiratet oder ledig, ob arm oder reich, über die Absicht seiner Reise etc. etc. So war es der Polizei möglich, die nötigen Massregeln rechtzeitig zu treffen.

Solche und ähnliche Methoden der geheimen Verständigung sind natürlich längst veraltet und durch die modernen Chiffriermethoden verdrängt worden. Doch will ich es nicht versäumen, einzelne ältere Methoden, die sich lange im Gebrauch erhielten und heute noch hie und da Anwendung finden können, näher zu besprechen.

I.

Gemischte Chiffrier-Methode.

Für jeden einzelnen Buchstaben und jede Ziffer lassen sich Zeichen setzen, die einer besonderen Sprache oder Wissenschaft entnommen sind; da in der Regel die aus einer Wissenschaft z. B. der Astronomie entnommenen Zeichen nicht hinreichend sind, um 24 Buchstaben zu bezeichnen, wird man sich aus verschiedenartigen Zeichen ein Alphabet zusammenstellen müssen.

Z. B.

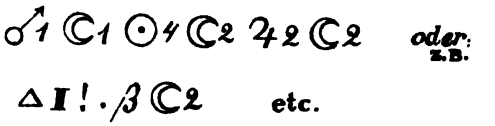
I	1 2 3 4	1 2 3 4	1 2 3 4	1 2 3 4	1 2 3 4	1 2 3 4
II	t z q i	r e h w	f x b v	a m s p	o g c u	l d n k
III	> □ – !	II · + ,	△ I V ;	: < ∮ =	η δ % ×	? β .. &
IV	☉	☾	♂	☽	♀	♃

Die Zeichen in der IV. Horizontalreihe sollen die Gruppen angeben, in welchen der zu chiffrierende Buchstabe (II. H.-Reihe) steht. Horizontalreihe I. und III. enthalten dann die Chiffrezeichen, die nach Belieben zu wählen sind.

*) Vgl. Klübers Kryptographik (1809) S. 296 ff.

Digitized by Google

Das Wort „Friede“, hiernach chiffriert, könnte so aussehen:



Es sind hier eine Menge Variationen möglich; immer wird man aber darauf bedacht sein müssen, denselben Buchstaben nie durch das gleiche Zeichen in einem Worte auszudrücken; im Interesse des Geheimnisses wird es auch liegen, möglichst viele sonstige verabredete graphische Zeichen als Nieten zwischen die geheimen Zeichen einzuschalten.

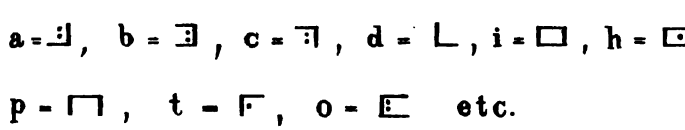
II.

Der Winkel- und Quadratchiffre (Maurerchiffre).

Die einzelnen Buchstaben können nun aber auch durch ganz willkürlich gebildete Figuren — unter Anwendung von geraden und gebogenen Linien — ausgedrückt werden. Chematisch lässt sich diese Art von Chiffrezeichen durch einige zusammengesetzte Figuren zeigen.

Z. B.

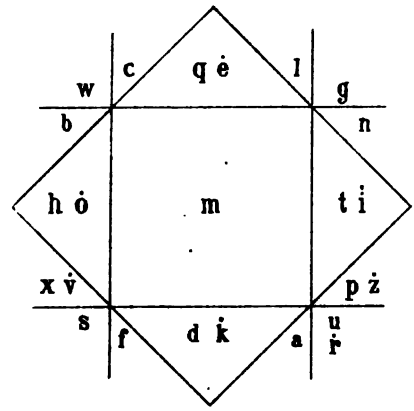
l	u̇	ä	g	k̇	d	r̈	n̈
m	v̇	b̈	i	ḣ	e	ẇ	ö
s	ẋ	c̈	p	q̇	f	ṫ	z̈

Nun ist 

Digitized by Google

Diese Figuren (Chiffrezeichen) sind also der Gesammtfigur entnommen und mit den entsprechenden Punkten versehen, die dort über den Buchstaben angebracht sind.

Winkel und Dreiecke werden z. B. durch folgende Figur eingeführt:



Also ist a=, b=, c=, d=, e=, i=, m= **etc.**

analog den Figuren des ersten Beispiels.

Ganz gleich ist auch „the heraldic cipher“ in J. H. Schoolings Aufsatz *), wo ein Wappenschild ähnlich eingeteilt ist wie die oben zuerst angegebene Figur.

Durch Einführung von Kreisfiguren in quadratische Zeichnungen können auch Kreissegmente und verwandte Figuren die Chiffrebuchstaben ersetzen. —

Aber auch abgesehen von diesen Angaben lassen sich andere ganz willkürlich geformte Figuren, die selbst wieder Bestandtheile bekannter Schrift- oder Drucktypen sein können, als geheime Chiffrezeichen verwenden; nur sind die schon mehrmals erwähnten Sicherheitsmassregeln auch hier nicht ausser Acht zu lassen. —

III.

Der Musik- oder Notenchiffre.

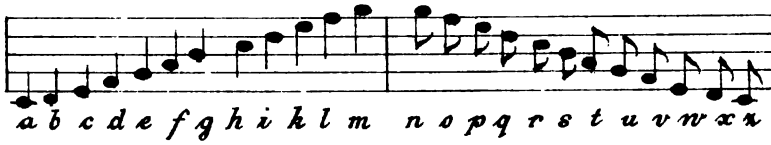
Bei diesem Chiffre werden die Buchstaben der geheimen Mitteilung durch Musikzeichen ausgedrückt. Diese Chiffriermethode

*) Vgl. die Litteraturangabe im Vorwort.

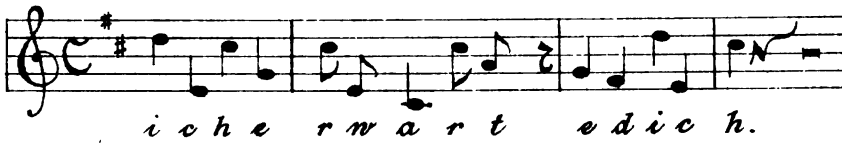
Digitized by Google

ist auch dazu geeignet, die Existenz einer geheimen Verständigung z. B. in der Abschrift einer musikgerechten Composition zu verbergen. Es ist aber klar, dass zur Anwendung dieser Methode vor allem auch theorisch-musikalische Kenntnisse erforderlich sind, da die als Chiffrezeichen verwendeten Musiknoten wie bei jedem Tonstück in Takte zu ordnen sind.

Hier will ich zum besseren Verständnis ein Beispiel aufzeichnen:



Die Mitteilung: „Ich erwarte Dich“ liesse sich beispielsweise so chiffrieren:



Eine so chiffrierte Mitteilung lässt sich ganz bequem zwischen die Takte einer bekannten Melodie einschalten.

Als Wechselzeichen bei gleichen Buchstaben eines Wortes lassen sich entweder noch andere Noten oder sonstige Zeichen, die in der Musiknotenschreibweise üblich sind, einführen.

Einen anderen Musikchiffre erwähnt Klüber in seinem Werke (S. 264 ff.); dort sind die Musiknoten in ein kreisförmiges Notensystem eingetragen — ähnlich den Chiffrezeichen im Circularscheibenchiffre, I. Abschnitt, Methode XII. —

IV.

Chiffriermethoden unter Anwendung von geraden und gebogenen Linien, sowie von Polygonen. — Punktier-Methoden. —

In diesem Capitel will ich einige wenn auch ältere, so doch ganz interessante Chiffriermethoden besprechen, die sich auch heute noch unter Umständen praktisch anwenden lassen.

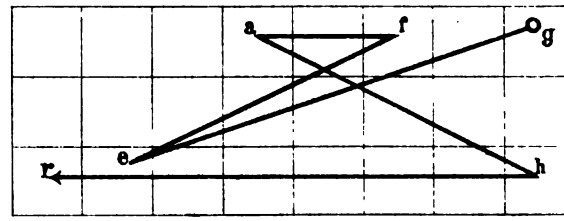
Digitized by Google

k	t	l	a	x	f	q	g
m	u	d	s	b	o	p	w
r	e	n	z	i	c	v	h

1. Dies sei beispielsweise ein Schlüssel, wie er im Besitz beider Correspondenten sein muss, abgesehen davon, dass diese sich einen solchen genau nach Verabredung zu jeder Zeit bilden können.

Zur Chiffrierung der geheimen Mitteilung zieht nun der Schreiber unter Berücksichtigung der Reihenfolge der zu chiffrierenden Buchstaben ohne Unterbrechung von einem Quadrate (der Tabelle) zum andern eine gerade Linie, wobei er den Anfang und das Ende der chiffrierten Mitteilung dem Empfänger kennzeichnet.

Also:



Diese Linienfigur wird dann (ohne jede Hilfslinie der Quadratzeichnung) in Originalgrösse dem Correspondenten übersandt, der die Eckpunkte dieser Figur mit seiner Tabelle (Schlüssel) vergleicht, wobei er sofort sieht, welche Buchstaben an die verschiedenen Ecken zu setzen sind.

Klüber gibt in seinem Werke (S. 288) ein Beispiel an, in welchem er statt der Quadrate concentrische Kreise benutzt.

---

2. Verwandt mit vorstehender Chiffriermethode ist eine andere, bei welcher die Chiffrebuchstaben durch irgend eine Punktierart so angedeutet werden, dass die örtliche Entfernung der Chiffrezeichen deren Bedeutung bedingen. Diese örtliche Entfernung kann selbst wieder bedingt sein durch die Verschiebung eines beweglichen Alphabetes (Fig. a.) über ein Papier hin, wobei jeweils

Digitized by Google

der betreffende Chiffrebuchstabe im Papier einpunktiert (Fig. b.) oder durch gemessene Abstände der Chiffre- bezw. Punktierzeichen von einander (siehe Massstabchiffre sub 3) gekennzeichnet wird. —

Ein Beispiel der ersten Art ist folgendes:

Fig. a.

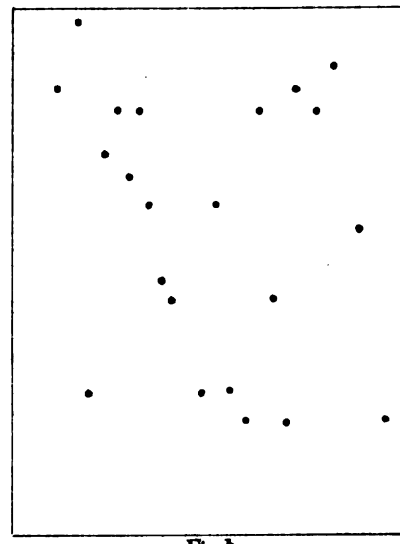


Fig. b.

Das Verfahren beim Chiffrieren ist nun dieses: Ein Papierstreifen wird nach Fig. a. mit dem Alphabet versehen, sodann wird dieser Streifen von irgend einer Seite des Papiers aus (in Fig. b. von der linken aus) über dieses hinweggeschoben, wobei man bei jedem Chiffrebuchstaben einen Punkt auf das Papier einzeichnet. Es wird also bei jedem Buchstaben (der geheimen Mitteilung) der Papierstreifen etwas vorwärts bewegt, sodass in einer Vertikalreihe nie mehr als ein Punkt eingezeichnet wird. Die einpunktierte Geheimschrift in Fig. b. lautet:

„Das Geheimnis ist entdeckt".

Nun lassen sich mit der in Fig. b. einpunktierten Geheimschrift verschiedene Variationen vornehmen, indem man die einzelnen Punkte durch gerade oder winkelige Linien mit einander verbindet, oder indem man die einzelnen Punkte als Ecken von Polygonen verwendet, sodass dadurch der Verdacht einer Geheimschrift möglichst gemindert werden kann. Ich will hier einige Beispiele anführen.

Digitized by Google

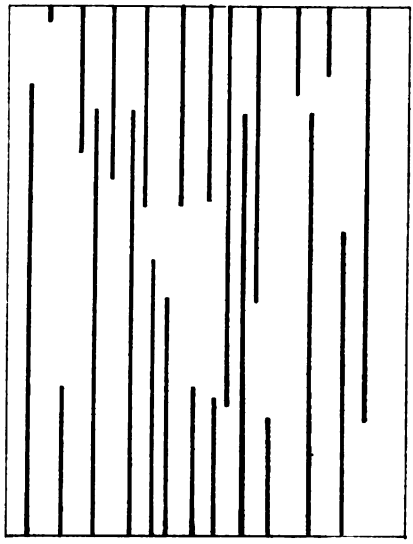


Fig. c.

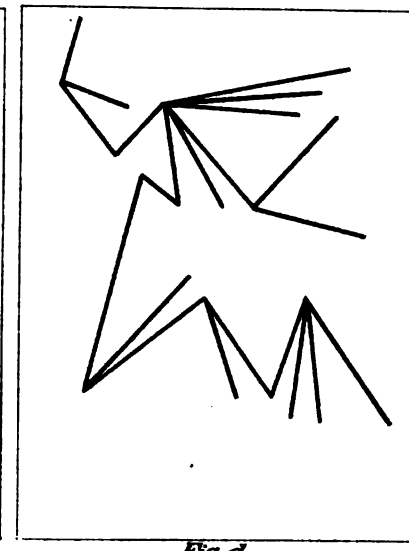


Fig. d.

Aus Fig. d. ist ersichtlich, dass durch Ergänzung weiterer Linien Polygone entstehen, die man durch Tinte oder Farbe ganz ausfüllen kann. Bei der Dechiffrierung solcher und ähnlicher Figuren ist stets wie bei Fig. b. zu verfahren. (Fig. c. und Fig. d. enthalten dieselbe Geheimschrift wie Fig. b.) Wenn man die Punkte von Fig. b. nach der am Anfang dieses Kapitels besprochenen Methode (sub 1) verbindet, so erhält man eine blitzartig gezackte Figur. In diesem Punkte ist auch diese Methode mit jener verwandt; denn die Bezeichnung eines bestimmten Buchstabens ist durch die Länge einer geraden Linie gebildet, jeder Winkel bezw. jedes Eck der Figur verweist auf einen bestimmten Buchstaben. —

---

3. Das Prinzip, dass die Länge einer geraden Linie die Bezeichnung eines gewissen Buchstabens bestimmt, ist auch gewahrt in dem sog. Massstabchiffre. Es wird ein Stäbchen (oder ein Papierstreifen) in 24 gleich grosse Felder eingeteilt, und diese werden mit den 24 Buchstaben des Alphabetes ausgefüllt. Hierauf wird die Entfernung der einzelnen Buchstaben der geheimen Mitteilung jeweils von dem einen Endpunkt des Stäbchens aus abgemessen und auf einem Papier einpunktiert (ähnlich wie in voriger Methode bei Fig. b.) Die Variationen der vorigen Methode lassen sich auch hier mit der einpunktierten Mitteilung verbinden.

Digitized by Google

Bei diesem Chiffre tritt aber noch eine neue interessante Variation hinzu. Es lassen sich nämlich die einzelnen abgemessenen Entfernungen auch an einem Faden durch Punktierzeichen erkenntlich machen; als Punktierzeichen sind ausser Punkten mit Tinte auch Knoten im Faden selbst zu verwenden. (Vergl. hierzu den unten folgenden Fadenchiffre.)

Will man vermeiden, dass gleiche Buchstaben nicht durch gleich grosse Entfernungen ausgedrückt werden, so rate ich an, die Weite der einzelnen Felder auf dem Massstab zwischen 1 und 2 ctm zu wählen, sodass z. B. die Entfernung von einem Endpunkt bis zu einem gewissen Buchstaben mit 7, 7,1, 7,3 . . . 7,9 oder 8, 8,1, 8,2 . . . 8,9 ctm punktiert werden kann, weil das betreffende Feld, in dem der Buchstabe eingezeichnet steht, vom 7. bis 9. ctm reicht. Statt der Dezimalzahlen können auch Bruchzahlen eingeführt werden, z. B. $8^1/_{10}$, $8^1/_5$ etc. (ctm,) wenn die geheime Mitteilung in Gestalt einer Zahlengeheimschrift dem Correspondenten übersandt werden soll. Vgl. ausserdem hierzu Methode XXV. im ersten Abschnitt.

---

4. Zu dieser Gruppe von Punktiermethoden gehört auch der sog. Fadenchiffre. Auf dem oberen Rand eines Kartons (oder Brettchens) werden die 24 Buchstaben des Alphabets aufgezeichnet und neben jedem Buchstaben vertikale Linien bis zum anderen Ende des Cartons gezogen. Ausserdem wird der linke und rechte Rand des Cartons mit kleinen spitzwinkeligen Einschnitten versehen, die dazu bestimmt sind, einem um den Carton zu wickelnden (weissen) Faden einen Halt zu geben. Der Faden wird links oben im Carton befestigt und sodann über die seitlichen Einschnitte um den Carton gewickelt. Hierauf folgt die Einzeichnung der Buchstaben der geheimen Mitteilung in der Weise, dass bei jedem Buchstaben ein Punkt oder kleiner Querstrich mit Tinte auf den Faden gezeichnet wird in der jenem Buchstaben entsprechenden Vertikalkolonne. Dieser Querstrich oder Punkt darf aber nie in der gleichen Horizontallinie links vor den anderen angebracht, sondern es muss jeweils eine Horizontallinie tiefer gerückt werden, sobald man rechts von dem zuletzt gemachten Punkt (oder Strich) in der gleichen Reihe keinen anderen mehr anzubringen hat.

Ist die ganze Mitteilung auf diese Weise eingezeichnet, so wird der punktierte Faden von dem Carton abgelöst und, als

Digitized by Google

Knäuel zusammengewickelt, dem Correspondenten übermittelt, der den Faden dann in gleicher Weise auf einen entsprechend präparierten Carton aufwickelt, um die Mitteilung bequem ablesen zu können.

Im Prinzip ist das Punktierverfahren das gleiche wie bei Methode IV. (zweiter Abschnitt) 2. Teil Fig. a. und b.

V.

Der Kartenchiffre.

Erste Art: Die geheime Mitteilung wird auf die Rückseite der Karten eines Spieles, die nach einer verabredeten Reihenfolge zusammengelegt sind, in der Weise aufgezeichnet, dass bei jedem Buchstaben die folgende Karte zur Aufzeichnung vorgenommen wird; hat die Mitteilung mehr Buchstaben, als Karten vorhanden sind, so wird — bei der ersten Karte wieder beginnend — der nächste Buchstabe neben oder unter den früher geschriebenen Chiffrebuchstaben gesetzt. Ist so die Mitteilung ganz aufgezeichnet, dann werden die Karten nach Belieben gemischt; der Empfänger der Karten, der die ursprüngliche Reihenfolge kennt, wird bequem die Mitteilung entziffern können. —

Zweite Art: Die Ränder der Karten werden „beschnitten", und nachdem die Karten, nach Verabredung geordnet, (mit einer Presse) zusammengepresst sind, werden die Chiffrezeichen auf den „Schnitt" der Karten geschrieben und diese hierauf gemischt, wodurch die geschriebenen Zeichen in viele kleine unmerkliche Bestandteile zerlegt werden.

Verwandt mit dieser letzten Art ist die Methode der Lacedaemonier, bei der ein Papierstreifen auf ein Stäbchen aufgerollt wird; über die auf- bezw. nebeneinanderliegenden Ränder hinweg wird die schmale Seite des Streifens mit den Chiffrebuchstaben beschrieben, der Länge des Stäbchens entsprechend. Nach dem Abnehmen des Papierstreifens erscheinen die Buchstaben, aus dem Zusammenhang gebracht, auf ganz verschiedenen Stellen des Streifens. —

Digitized by Google

VI.

Sympathetische Tinten.

Unter sympathetischer Tinte ist eine solche Flüssigkeit zu verstehen, mit welcher die Chiffrezeichen aufgezeichnet werden, ohne dass die geschriebenen Zeichen zum Vorschein kommen, welche auch nicht eher gelesen werden können, als bis ein Mittel angewendet wird, das den unsichtbaren Zeichen eine Farbe verleiht. Kasiski*) gibt in seinem Werkchen die Herstellung sechs verschiedener Arten von sympathetischen Tinten an. Zum Vorschein kommen die mit solchen Tinten geschriebenen Zeichen teils dadurch, dass man die Schrift der Wärme oder der Luft aussetzt, teils dadurch, dass man sie mit einer färbenden Substanz — wie Pulver — oder mit Wasser oder mit einer anderen Flüssigkeit in Verbindung bringt. —

Heutzutage ist der Gebrauch sympathetischer Tinten als Geheimschriftmittel ziemlich verdrängt worden durch andere bewährte Geheimschriftmethoden; ihre Anwendung ist jetzt nur noch da zu finden, wo es sich um kleine Kunststücke handelt. —

Höchstens bei Punktier-Methoden lässt sich die Anwendung sympathetischer Tinten (zur geheimen Punktierung der Chiffrebuchstaben) empfehlen. —

Eine ganz neue Erfindung sei hier noch erwähnt: Zur Imprägnierung des Papiers verwendet man eine Lösung von Haroidsalzen des Kobalts und schreibt auf das so präparierte Papier mit einer Lösung von Kochsalz. Beim Erwärmen des Papiers werden die Schriftzeichen sichtbar, während sie beim Erkalten verschwinden. —

Von den Geheimschriftmethoden dieses Abschnittes sind die unter Nr. IV. besprochnen Chiffremethoden sowie der Musikchiffre (Methode III.) auch heute noch zur Anwendung zu empfehlen; ihre interessante Originalität spricht auch entschieden dafür. — Die sonstigen Methoden in diesem Abschnitte sind zumeist veraltet und der Umständlichkeit wegen weniger wie jene zu empfehlen; sie wurden nur der Vollständigkeit halber hier erwähnt. —

*) Kasiski, die Geheimschriften etc. (Berlin 1863) S. 4 ff.

Digitized by Google

Dritter Abschnitt.

Kryptographie und Graphologie*).

Bei der gegenwärtig noch herrschenden Unklarheit über „Graphologie“ (Handschriften-Deutungskunde) möchte ich zunächst in einigen Worten meine Stellung zu dieser jungen Wissenschaft darlegen. —

Von den vielen „Handschriften-Deutern“, die in den Zeitschriften ihre Dienste anpreisen, sind die meisten nur sehr dilettantenhaft vorgebildet. Seit dem Erscheinen von Professor Preyer's „Psychologie des Schreibens“ hat sich aber in Deutschland eine Gesellschaft für wissenschaftliche Graphologie gebildet (1896), an deren Spitze Graphologen wie Hans H. Busse, Dr. Ludwig Klages, Dr. med. Georg Meyer stehen. Der Sitz dieser „Deutschen graphologischen Gesellschaft“ ist München; hier wohnte ich auch den gründlichen wissenschaftlichen Graphologie-Unterrichtskursen des Herrn Hans H. Busse bei, dem ich ausserdem noch manche wertvolle Anregungen über die Bedeutung der Graphologie für die Kryptographie verdanke.**)

Diese Worte mögen genügen über Graphologie im allgemeinen.

Nun noch einige Worte über die angewandte Graphologie.

Die nächstliegende und häufigste Anwendung der Graphologie ist die Beurteilung des Charakters eines Menschen nach seinen Schriftzügen. In dieser Hinsicht vermag die Graphologie dem privaten wie geschäftlichen Verkehr manche gute Dienste zu leisten, so besonders bei Prüfung von persönlichen Dienstofferten,

*) Vgl. hierzu meinen Aufsatz: Die Graphologie als Hilfsmittel zur Entdeckung von Geheimschriften — veröffentlicht in den „Graphologischen Monatsheften“ Nr. 4 und 5 (1899), Schülers Verlag, München. —

**) Wer sich näher mit der wissenschaftlichen Graphologie beschäftigen will, den verweise ich auf die bereits citierten „Graphologischen Monats-Hefte“ und auf die Werke von Hans H. Busse: „Bibliographie der Graphologie“ (München 1900. 1.— Mk.) und „Die Handschriftendeutungskunde. Ein Unterrichtskursus.“ (2. Aufl., München 1900. 8.— Mk.)

Digitized by Google

ferner bei Erforschung des Charakters einer historischen Persönlichkeit; sodann gewinnt man mit ihrer Hilfe manche interessante Beiträge zur „Psychologie des Weibes", das ja noch viele ungelöste Probleme in sich birgt. Ebenso lässt sich die Graphologie mit gutem Erfolg auf dem Gebiete der „Criminalpsychologie" dienstbar machen. Welchen Wert die Graphologie als paedagogisches Hilfsmittel hat, ersehen wir aus einem Aufsatze des verdienstvollen Paedagogen Chr. Ufer: „Schrift und Individualität bei Kindern" (im encyklopaed. Handbuch der Paedagogik, herausgegeben von W. Rein 1898). — Auch bei der Untersuchung der Echtheit von Autogrammen spielt die Graphologie eine gewisse Rolle. — Die allerwichtigste Anwendung findet die Graphologie auf dem Gebiete der gerichtlichen Schriftexpertise, bei der sie die unbedingte Grundlage zur Untersuchung von Handschriftenverstellungen und -Fälschungen bildet. —

Wie dieser Abschnitt darthun soll, findet die Graphologie auf dem Gebiete der Geheimschriftenkunde eine ganz neue nicht zu unterschätzende Anwendung.

Eine von John Holt Schooling in „the pall mall magazine" (1896) veröffentlichte Geheimschrift eines russischen Nihilisten [1]), der rein graphische Eigenheiten dazu benutzte, seine geheime Mitteilung in einigen ganz harmlosen Zeilen zu verbergen, veranlasste mich zu eingehenderen Untersuchungen auf dem Gebiete der Kryptographie, gestützt auf graphologische Kenntnisse. Es wunderte mich übrigens, dass Schooling, der selbst Graphologe ist, bei Erörterung jener Geheimschrift keine Stellung nahm zur Graphologie als wichtiges Hilfsmittel zur Entdeckung der Existenz einer geheimen Verabredung.

Bei näherer Prüfung der bis jetzt bekannten Geheimschriftmethoden konnte ich vier Methoden aus ihrer Reihe ausscheiden, bei denen die Graphologie als Hilfsmittel zur Entzifferung bezw. zur Entdeckung der Existenz einer geheimen Mitteilung mit Nutzen herangezogen werden kann. Es sind dies nämlich: Fleissners neue Patronengeheimschrift [2]), der Netz- oder Gitterchiffre [3]), Boetzel's Methode [4]) und die oben schon erwähnte Geheimschrift eines Nihilisten.

---

[1]) Vgl. I. Abschnitt, Methode XVIII. —
[2]) Vgl. I. Abschnitt, Methode XI.
[3]) Vgl. I. Abschnitt, Methode X.
[4]) Vgl. III. Abschnitt, Capitel III.

Digitized by Google

Nachstehend will ich in einzelnen Capiteln diese vier Geheimschriftmethoden vom graphologischen Standpunkt aus betrachten und analysieren.

An diese Capitel will ich sodann einige Versuche anreihen, neue Geheimschriftmethoden auf graphologischen Prinzipien aufzubauen. —

In einem Anhang will ich schliesslich einige Anleitungen geben zur Bildung von Geheimschriften, bei denen selbst graphologische Kenntnisse nicht hinreichend sind zur Entdeckung der Existenz einer in harmlosen Zeilen verborgenen Geheimschrift. —

a) Die Graphologie als Hilfsmittel zur Dechiffrierung von Geheimschriften.[1]

I.

Fleissner's neue Patronengeheimschrift. [2]

Diese Chiffriermethode gehört zu jenen Geheimschriftmethoden, welche das Princip befolgen, die Buchstaben der mitzuteilenden Nachricht verabredeten Vorlagen gemäss in eine ungewöhnliche Reihenfolge zu bringen. Einige Momente können den Graphologen über die wahre Reihenfolge der zwar nebeneinanderstehenden, nicht aber in gewöhnlicher Schreibweise nebeneinandergesetzten Schriftzeichen Aufschluss geben.

Nachfolgend eine Anwendung dieser „Patronen"-Geheimschrift:[3]

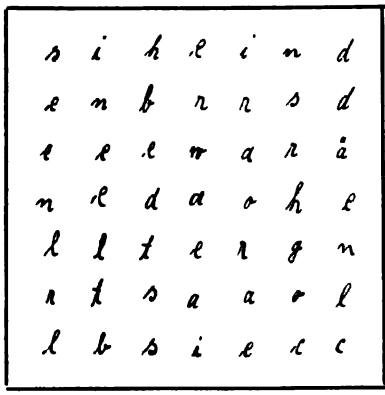


Fig. a.

1.	37 s	13 i	25 h	38 e	1 i	14 n	26 d
2.	27 e	2 n	15 b	28 r	39 r	40 s	3 d
3.	16 e	4 e	41 e	17 w	29 a	5 r	18 ä
4.	6 n	42 e	30 d	a	7 o	19 h	31 e
5.	48 l	32 l	8 t	44 e	20 r	33 g	45 n
6.	34 r	21 t	22 s	9 a	(46) a	35 o	10 l
7.	11 l	(47) b	36 s	23 i	12 e	(48) c	24 c

Fig. b.

[1]) Ueber andere Dechiffriermethoden vgl. vor allem die Werke von Fleissner (1881) und Kasiski (1863), die ich oben im Vorwort erwähnte.

[2]) Vgl. I. Abschnitt, Methode XI.

[3]) Genaue Untersuchungen liessen sich nur an Originalschriftstücken vornehmen.

Digitized by Google

Die Nummerierung der einzelnen Buchstaben (Fig. b.) gibt ihre zeitliche Entstehung an. Abgesehen von den bestimmten Abständen der Buchstaben, die ja sofort auf das Schreiben mit Hilfe einer präparierten (durchlöcherten) „Patrone“ schliessen lassen, kann der Graphologe hier mit einer gewissen Sicherheit die früher und die später entstandenen Schriftzeichen von einander unterscheiden, indem er bei genauer Untersuchung entdecken wird, dass die zuerst entstandenen Schriftzeichen mit einer grösseren Sorgfalt durch die Löcher der „Patrone“ geschrieben wurden, als die später und zuletzt entstandenen, bei denen sich der Schreiber schon etwas an den „behindernden Schreibumstand“ gewöhnt hat und so der gewohnten Schreibbewegung freieren, d. i. schnelleren Lauf lassen kann.

Vgl. die Hauptrichtungsänderung von *n* (2) Zl. 2 und von *n* (45) Zl. 5. Ein Uebergangsstadium zeigt *n* (14) Zl. 1. Vgl. ferner die drei nebeneinanderstehenden *e* Zl. 3; ferner *t* (8) Zl. 5 und *t* (21) Zl. 6. — Also die Hauptrichtung, die anfangs nach unten links geneigt ist, ändert sich gegen die Mitte der Schreibzeit senkrecht nach unten und schliesslich nach unten rechts. Vgl. weiter die grosse Aehnlichkeit der 3 *e*: *e* (38) Zl. 1, *e* (41) Zl. 3, *e* (42) Zl. 4, die zeitlich fast unmittelbar aufeinanderfolgen, gegenüber dem viel früher entstandenen *e* (4) Zl. 3. Vgl. ferner das mit Sorgfalt gemachte *r* (5) Zl. 3 und das später entstandene *r* (28) Zl. 2, oder *r* (39) Zl. 2 etc. etc. Aehnliche Resultate werden sich auch aus dem Vergleich der übrigen Buchstaben ergeben.

Man kann ferner die Beobachtung machen, dass die früher entstandenen Schriftzeichen in der Regel mehr Rundungen, die später entstandenen aber mehr Ecken aufweisen, da die ersten, mit grösserer Sorgfalt geschriebenen Schriftzeichen sich mehr der Schulvorlage anlehnen als die später, mit einer gewissen Schnelligkeit gesetzten Buchstaben. Vgl. *i* (1) Zl. 1, *n* (2) Zl. 2, *d* (3) Zl. 2, *e* (4) Zl. 3 etc. mit *b* (15) Zl. 2, *w* (17) Zl. 3, *ä* (18) Zl. 3 etc.

Hierher gehören auch noch fünf weitere Versetzungsmethoden nach welchen die Buchstaben der Klarschrift verabredeten Vorlagen gemäss in eine ungewöhnliche Reihenfolge gebracht werden. Diese sind nämlich:

Die hebräische und chinesische Methode, die Methode im Zickzack oder in der Schlangenlinie, die Methode in der Diagonale

Digitized by Google

und im Parallelogramm, die ich alle im ersten Abschnitt (Methode II bis V) näher erörtert habe.*)

Hat man eine nach diesen letztgenannten Methoden hergestellte Geheimschrift graphologisch zu untersuchen, so wird man wie bei der Patronengeheimschrift zu Werke gehen müssen, weshalb ich von einer weiteren Anleitung zur Untersuchung absehen kann. Nur will ich hier noch erwähnen, dass bei der hebräischen Methode, die ein Schreiben von rechts nach links fordert, auch die Zeilenrichtung in Frage kommt. Die Schrift eines Menschen, die in der Regel ansteigend ist, wird in diesem Falle, von links aus betrachtet, abfallend erscheinen und ebenso umgekehrt bei ursprünglich abfallender Zeilenrichtung. Bei den übrigen Methoden wird auch die Randbildung in Betracht zu ziehen sein, die teils auf den Anfang, teils auf die Art der Chiffrierung schliessen lassen kann.

Wenn auch die Ergebnisse einer so angestellten Untersuchung ziemlich gering scheinen, so darf man doch nicht ihren Wert für einen Dechiffreur unterschätzen, der bei der Entzifferung nach anderen Methoden noch viel minutiöseren Anhaltspunkten einen Wert beizulegen weiss. Wenn viele verschiedene noch so kleine Anhaltspunkte bei einer Dechiffrierung zusammenwirken, wird man zufrieden sein können: denn kleine Ursachen, grosse Wirkungen!

Der verminderte Nutzen der Graphologie auf diesem Untersuchungsgebiet liegt aber ganz wo anders; es werden nämlich in der Regel die nach obigen Methoden chiffrierten Mitteilungen nicht in ihrer ursprünglichen Form, sondern in Abschrift dem Correspondenten übermittelt. Aber immerhin wird die mit Hilfe der „Patrone“ geschriebene Mitteilung auch oft im Original übersandt, weil andernfalls der Empfänger zu viel Mühe hätte, die Buchstaben wieder in die richtigen Abstände von einander zu bringen, um seine „Patrone“ bei der Dechiffrierung verwenden zu können.

Ein höheres Interesse für den untersuchenden Graphologen erwecken alle jene Geheimschriftmethoden, die eine Verdeckung der geheimen Mitteilung in ostensiblen Schriftstücken anstreben. Auf diesem Gebiete kann er vielfach mit Erfolg belohnt werden. —

---

*) In weiterer Linie gehört auch die Versetzungsmethode VIII (I. Absch.) hierher; ebenso Methode XVI. (I. Absch.).

Digitized by Google

II.

Der Netz- oder Gitterchiffre.*)

Fleissner's neue Patronengeheimschrift, die auf dem Prinzip dieses Netzchiffres beruht, gibt uns schon die Tendenz dieser Chiffrierart zu erkennen.

Die Anwendung des Netzchiffres ist leicht ersichtlich aus der in Fig. b. dargestellten Zeichnung: durch die Quadrate und Rechtecke, die genau nach dieser Zeichnung**) aus einem Papier

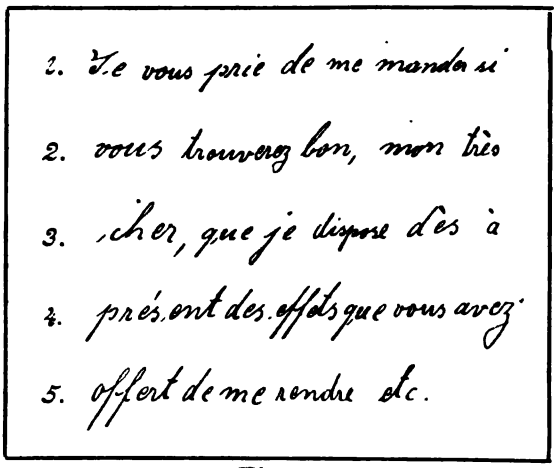


Fig. a.

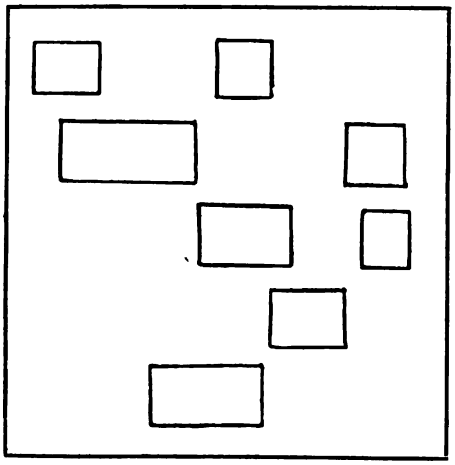


Fig. b.

*) Vgl. I. Abschnitt, Methode X.

**) Ueber die Herstellung anderer Netze vgl. Klüber's Kryptographik (1809) S. 192, ff.

Digitized by Google

oder Carton auszuschneiden sind, werden die einzelnen Wörter der geheimen Mitteilung auf ein untergelegtes Papier geschrieben, oder man legt auch eine solche Zeichnung wie ein Linienblatt unter das zu beschreibende Papier und schreibt die einzelnen Wörter der geheimen Mitteilung in die durchscheinenden Rechtecke und Quadrate. In die Zwischenräume werden nun andere beliebige Wörter derart eingefügt, dass sie mit den eingeflochtenen Wörtern der geheimen Mitteilung selbst wieder einen Sinn geben, der mit dem Sinn der geheimen Mitteilung natürlich in keinem Zusammenhang stehen darf. Die Construction einer solchen gleichgiltigen Mitteilung unter Anwendung der schon niedergeschriebenen Wörter ist aber keineswegs leicht, weshalb sich diese Methode für eine Geheimschrift auch sehr wenig empfiehlt.

Wir haben jetzt aber die graphologischen Momente zu betrachten, die auf das Vorliegen einer Geheimschrift in der ostensiblen Mitteilung schliessen lassen. Die geheime Mitteilung lautet: vous me (Zl. 1) trouverez très (Zl. 2) dispose (= disposé) à (Zl. 3) vous (Zl. 4) rendre (Zl. 5). —

Wenn man nun die graphologischen Grundsätze bezüglich der Zeilenrichtung ins Auge fasst, so muss man gestehen, dass durch das nachträgliche Ausfüllen der durch die geheimen Wörter schon fixierten Zeilen eine zeitliche Unterbrechung in ihnen bedingt ist, welche ein Variieren in der Zeilenrichtung zur Folge hat. Vgl. die Unterbrechung zwischen *que* und *vous* (Zl. 4) ferner zwischen *me* und *rendre* (Zl. 5) etc.

Von grösserer Wichtigkeit ist aber die Verschiedenheit der Neigungswinkel der Hauptrichtungen der geheimen Wörter im Verhältnis zu den später geschriebenen Ergänzungswörtern. Man beachte die ziemliche Steilheit der zuerst geschriebenen Buchstaben, namentlich das *u* in *vous* (Zl. 4) und das *n* und zweite *r* im Worte *rendre* (Zl. 5), wo der Neigungswinkel genau 90^0 beträgt. Damit vergleiche man die später erfolgte Aufzeichnung der Wörter, die im Verhältnis zu jenen auffallend schräg sind: z. B. *prie* und *de* gegenüber *vous* (Zl. 1), *je* (Zl. 3) gegenüber *dispose* (Zl. 3), ferner *effets que* (Zl. 4) gegenüber *vous* (Zl. 4), *offert de me* (Zl. 5) gegenüber *rendre* (Zl. 5). —

Als weiteres wichtiges Moment für die Untersuchung tritt die Schriftweite hinzu. Die Quadrate und Rechtecke durch bezw. in welche die geheimen Wörter geschrieben werden, zwingen den Schreiber dazu, das einzelne Wort enge zu schreiben, damit der

Digitized by Google

zu Verfügung stehende kleine Raum ja nicht überschritten werde, während beim Ausfüllen der Lücken der Schreiber bestrebt ist, die Buchstaben weit auseinanderzuziehen, um die Zwischenräume zwischen den früher und später geschriebenen Wörtern nicht auffallend erscheinen zu lassen.

Vgl. z. B. *vouz* und *trouverez* (Zl. 2), ferner *cher que je* und *dispose* (Zl. 3).

Im Prinzip werden aber auch die Zwischenräume zwischen den früher und später geschriebenen Wörtern selbst als Indizien einer versteckten Geheimschrift gelten können, zumal wenn weniger Sorgfalt und Vorsicht beim Ausfüllen der Lücken aufgewendet wurde.

Wie ich schon oben erwähnte, ist die Anwendung dieser Geheimschriftmethode nicht gar so einfach, da die Grenze der verfügbaren Wörter und Phrasen bei der Ergänzung der Lücken sehr enge gezogen ist, sodass in der Regel schon der gezwungene Satzbau und der auffallende Gebrauch gewisser Wörter, die für den Sinn der vorliegenden bedeutungslosen Mitteilung durchaus entbehrlich wären, grossen Verdacht auf ein verdecktes Geheimnis begründen können *).

Wenn man bei der Untersuchung einer derartigen Geheimschrift alle diese Momente genau berücksichtigt, so wird man sicher zu einem befriedigenden Resultat kommen müssen. Während bei den vorhergehenden und nachfolgenden Geheimschriftmethoden in der Regel nur die Existenz einer verborgenen Geheimschrift mit Hilfe der Graphologie zu entdecken ist, können aber bei diesem Netzchiffre graphologische Momente das ganze Geheimnis klarlegen. —

III.

Boetzel's Methode **).

Der Gedanke, dem Correspondenten in einem ostensiblen Schriftstücke die Chiffrebuchstaben auf irgend eine „geheime" Weise erkennbar zu machen, hat Boetzel dahin geführt, durch absichtliche Correcturen an Buchstaben die geheimen Chiffrezeichen anzudeuten.

*) Vgl. hierzu Heidels Punktier-Methode, I. Abschnitt, Methode XXVII dieses Werkchens.

**) Veröffentlicht in der Zeitschrift: „Ueber Land und Meer" (1899, Nr. 1).

Digitized by Google

Die erfolgreiche Verwendung solcher Correcturen ist Boetzel aber etwas missglückt, wenn er den Umstand, dass man sich beim Schreiben zuweilen „verschreibt", als Mittel zur Kennzeichnung von Chiffrebuchstaben verwendet und des näheren vorschlägt, bei einer beliebigen Mitteilung (oder Abschrift) in Klarschrift die einzelnen Buchstaben der geheimen Mitteilung durch eine absichtliche Correctur von Wortanfangsbuchstaben erkennbar zu machen. Mir ist es nicht klar, warum denn bloss die Anfangsbuchstaben und nicht auch andere zu solchen Correcturen verwendet werden sollen. Man stelle sich nur einmal ein grösseres Schriftstück vor, in welchem mehrere Correcturen von Buchstaben nur am Wortanfang und nie an einer anderen Stelle des Wortes auftreten. Ich glaube, man braucht keine besondere graphologische Kenntnisse zu besitzen, um das eigenartige Auftreten solcher Correcturen auffallend zu finden. Es wäre doch sicherlich weniger auffallend, die Correcturen auch an beliebig anderen Stellen eines Wortes — wo nur möglich — vorzunehmen. Aber auch in diesem Falle wird es dem Graphologen keine schwierige Aufgabe sein, die absichtlichen Correcturen von unwillkürlichen zu unterscheiden und somit auf die Existenz einer Geheimschrift zu schliessen. —

Nachstehend eine Anwendung der Boetzel'schen Methode:

1. Mit fremden Menschen nimmt man sich zusamen,
2. da merkt man auf, da sucht man seinen Zweck
3. in ihrer Gunst, damit sie nützen sollen; allein
4. bei Freunden läßt man frei sich gehn, man
5. irrt in ihrer Liebe, man erlaubt sich eine Laune
6. ungezähmter wirkt die Leidenschaft, und so ver-
7. letzen wir am ersten die, die wir am zartesten
8. lieben. — (Goethe.)

Digitized by Google

Um die Correctur an den einzelnen Buchstaben vorzunehmen, wird man nach dem allgemeinen Prinzip verfahren müssen, dass bei mittleren Buchstaben (z. B. a, e, n etc.) die Kennzeichnung durch diese überragende Buchstaben (z. B. f, t, g etc.) geschehen muss und ebenso umgekehrt.

Bei der Untersuchung dieser Correcturen hat man vor allem ihre Entstehung zu prüfen und sich die Frage vorzulegen: Ist es wahrscheinlich, dass der Schreiber an dieser Stelle zuerst einen langen Buchstaben setzen wollte und ihn dann — weil unrichtig — durch einen mittleren Buchstaben corrigierte, oder umgekehrt den fälschlicherweise schon ganz oder teilweise niedergeschriebenen mittleren Buchstaben durch einen langen ersetzte? —

Im allgemeinen dürfte jemand, der die Schrift gut beherrscht, während des Niederschreibens eines Wortes weniger an die Schreibbewegung als an den Inhalt des zu schreibenden Satzes denken. Somit wird ein unwillkürliches „Verschreiben" nur da entstehen können, wo der Schreiber entweder gedankenlos schreibt (z. B. beim Abschreiben), oder wo die Gedanken des Schreibers vorauseilen und an irgend einem später zu schreibenden Worte haften bleiben. Dieses letztere „Verschreiben" erkläre ich mir so, dass der Schreiber, um nicht seine vorauseilenden Gedanken zu verwischen, die Schnelligkeit seines Schreibens der seines Denkens unwillkürlich anpasst und so eine Reihe von Buchstaben oder Wörtern überfliegt und mit dem zuletzt gedachten Worte weiterfahren will. Analog ist auch die Verbesserung eines Buchstabens, der fast unmittelbar vorher richtig niedergeschrieben, aber bei der dem nachdenkenden Geiste vorauseilenden Schrift falsch gesetzt wurde. Merkwürdigerweise treten solche Correcturen meistens am Anfange (d. i. am 1. oder 2. Buchstaben) einer Silbe auf, weil nämlich eine früher oder später vorkommende Silbe, die man im Geiste festhält, ähnlich- oder gleichlautend beginnt. —*)

Wer diese Umstände bei einer Untersuchung in Betracht ziehen wird, den kann ein absichtliches „Verschreiben" nicht so leicht täuschen, zumal wenn er die betreffende Correctur stets mit verwandten Momenten in der Handschrift vergleicht.

Wenn man also — was doch die Regel ist — das niederzuschreibende Wort, das z. B. mit *en* endigt, in Gedanken festhält,

*) Vergl. auch meinen Aufsatz: „Der Einfluss intensiver Geistesthätigkeit auf die Handschrift. (Schreibfehler und Correcturen.)" in den „Graphologischen Monatsheften", 1899 No. 6/7. S. 106.

Digitized by Google

so wird man bei dem *e* oder *n* (bei der Schreibbewegung) wohl nicht in die Höhe fahren, um beispielsweise ein *f* oder *t* zu schreiben, das nach dem Sprachgebrauch überhaupt nie in diesem Worte vorkommen könnte. Vgl. die Wörter *und* (Zl. 6), *ersten* (Zl. 7), in welchem Worte der Bogen unten z. B. auf ein *a, o, d* oder *g* schliessen lässt, wogegen aber einer solcher Buchstaben niemals in diesem Worte vorkommen kann. Ferner ist zu erwägen, dass bei einer Handschrift, die ziemlich fliessend ist, eine absichtliche Correctur die natürliche Schreibbewegung bedeutend mehr hemmt, als eine unwillkürliche. Wenn sich z. B. der Schreiber in der Mitte oder am Ende eines Wortes erst überlegt, wie er an dem betreffenden Buchstaben die Correctur am besten anzubringen hat, während derselbe Buchstabe an einer anderen Stelle im gleichen oder ähnlichen Zusammenhang ganz zwanglos d. h. ohne Correctur niedergeschrieben wurde, so wird jener corrigierte Buchstabe sicher ganz unnatürlich, gekünstelt und daher für den vergleichenden Graphologen auffallend erscheinen. Vergleiche die Wörter *lieben* (Zl. 8) und *Menschen* (Zl. 1), ferner *seinen* (Zl. 2) und *zusammen* (Zl. 1), *sollen* (Zl. 3) und *allein* (Zl. 3) nach den beiden *e*, sodann *wirkt* (Zl. 6) und *merkt* (Zl. 2), *und* (Zl. 6) und *ruht* (Zl. 5), während die übrigen *u* keine Spuren von einer Correctur zeigen.

Aus solchen und ähnlichen Vergleichen, sowie unter Erwägung der Entstehung der fraglichen Correctur wird der Graphologe stets ein Resultat bei der Untersuchung gewinnen können. —

Was die Boetzel'sche Methode an und für sich betrifft, so kann ich nicht sagen, dass sie vollständig neu ist, denn sie beruht doch im Prinzip nur auf der alten Punktiermethode von Schotti*); Boetzel wählt statt jener von dem einzelnen Buchstaben unabhängigen Punktierzeichen Correcturen, die direkt mit dem fraglichen Buchstaben in Verbindung stehen, er verwendet also zu Punktierzeichen rein graphische Eigenheiten. Einzelne Correcturen mögen ja ganz geschickt angebracht werden können, aber niemals sämtliche. —

Man könnte nun aber doch dem Graphologen die Arbeit bei der Untersuchung etwas erschweren, wenn man einer Correctur den Anschein einer natürlichen Begründung gäbe, indem man — das Symptom eines vorauseilenden Denkens erheuchelnd — den Wortanfangsbuchstaben eines später folgenden Wortes fälschlich

*) Vgl. Methode XXVI. Abschnitt I.

Digitized by Google

unmittelbar vor ein früheres Wort setzt und wieder ausstreicht, ohne ihn jedoch dadurch unkenntlich zu machen.

Diesem, für das Auge des Nichteingeweihten höchst wertlosen durchstrichenen Buchstaben kann man aber viele geheime Bedeutungen beilegen: er kann nämlich einmal selbst den betreffenden Chiffrebuchstaben darstellen, oder er kann darauf hinweisen, dass der 1., 2., 3. etc. vorausgehende oder nachfolgende Buchstabe als Chiffrebuchstaben zu gelten habe, oder aber er kann die gleiche Bedeutung demselben Buchstaben einer späteren oder früheren Silbe, eines späteren oder früheren Wortes übertragen u. s. f.

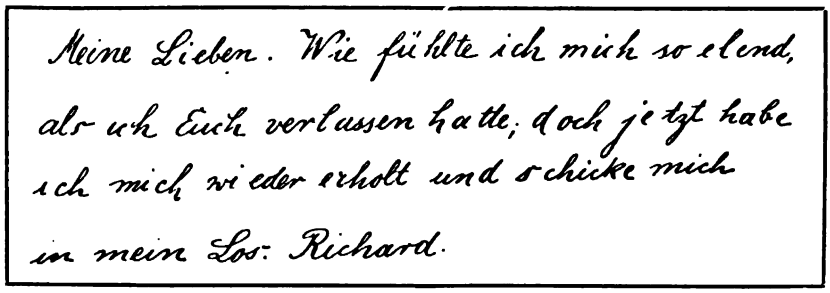
Den nämlichen Erfolg kann man erzielen, wenn man die Correctur eines Buchstabens wegradiert und dann den verschiedentlich vorgenommenen Radierungen eine geheime Bedeutung anweist. Auch ein Wechseln mit Correcturen und Radierungen dürfte für solche kryptographische Zwecke von Nutzen sein, namentlich wenn man auffallende Correcturen einfach durch Radierungen ersetzt.*)

IV.

Geheimschrift eines Nihilisten**).

Dem scharfsinnigen Nihilisten und Verbrecher gelingt es, selbst den wachsamsten und erfahrensten Aufsichtsbeamten zu hintergehen, um seinem Complicen durch die Hand des Beamten eine geheime Nachricht zukommen zu lassen, was nachstehendes Beispiel einer Geheimschrift beweist.

Fig. a.



*) Ueber andere Möglichkeiten graphischer Kennzeichnung von Chiffrebuchstaben vgl. das nächste Capitel.

**) Veröffentlicht in „the pall mall magazine“ (1896). Dazu vgl. oben Abschnitt I, Methode XVIII.

Digitized by Google

In dieser harmlosen Mitteilung ist eine geheime Ordre versteckt. Die für den Laien unauffällige Verdeckung des Geheimnisses bewirkt nun, dass der Brief ohne jeden Verdacht durch die Hände des Aufsichtsbeamten weiterbefördert wird. Liessen gewisse Zeichen den Beamten darauf schliessen, dass man es in dem speziellen Falle mit dem Versuch einer geheimen Verständigung zu thun hätte, so würde er natürlich dieses Schreiben zurückhalten und einer näheren Prüfung unterziehen. Dass dabei volle Klarstellung des Geheimnisses erreicht würde, ist freilich kaum anzunehmen, da zumeist eine Combination mehrerer Geheimschriftmethoden die Grundlage des eigentlichen Geheimnisses bildet. Es würde aber auch schon die Entdeckung der Existenz einer geheimen Mitteilung in den harmlos klingenden Zeilen genügen, um die Beförderung desselben und damit auch die strafbaren Pläne solcher Individuen zu vereiteln. —

In der obigen Geheimschrift (Fig. a) sind nun drei verschiedene Methoden mit einander verbunden. Die eine Methode

Fig. b.

(Zehner) \ (Einer)	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

Fig. c.

51 = v	31 = l
15 = e	31 = l
42 = r	15 = e
33 = n	12 = b
24 = i	42 = r
13 = c	24 = i
23 = h	15 = e
44 = t	21 = f
15 = e	15 = e
11 = a	

Fig. d.

5 1 : 1 5 : 4 2 : 3 3 : 2 4 : 1 3 : 2 3
Meine L i ebenw iefü hl tei chm ic hsoe l end al sic

4 4 : 1 5 : 1 1 : 3 1 : 3 1 : 1 5 : 1 2 : 4 2
heuc hver l assen h a tte d och j e tztha b ei chmi ch

2 4 : 1 5 : 2 1 : 1 5
wi eder e rholt un d s chick emichinmeinlosrichard.

— Fig. b — versetzt die Buchstaben der geheimen Mitteilung nach Art des sog. Multiplicationschiffres (vgl. Methode VI im I. Abschnitt); Fig. c gibt das Resultat dieser Versetzung an.

Digitized by Google

Die stellvertretenden zweistelligen Zahlen werden aber selbst wieder ausgedrückt durch einzelne Buchstabengruppen, die ihrem Gliederumfange nach den Zehnern bezw. Einern jener Zahlen entsprechen; vgl. Fig. d. —

Die dritte Methode hat nun die Aufgabe, diese Buchstabengruppen in dem Originalschriftstück dem Empfänger desselben erkennbar zu machen. Wie das geschieht, ist aus der Besprechung dieser Geheimschrift oben in Methode XVIII, I. Abschnitt zu ersehen.

Betrachtet man die einzelnen Wörter in Fig. a etwas näher, so müssen sofort die häufigen Unterbrechungen innerhalb eines Wortes auffallen; sie sind auffallend insofern, als sie keineswegs überall natürlich genug erscheinen. Ausserdem sind sie an entsprechenden Stellen nicht consequent durchgeführt, z. B. die an und für sich begründete Unterbrechung nach einem *i*-Grundstrich, um den *i*-Punkt sofort zu setzen, in den Wörtern *Lieben, ich* (Zl. 1), *jetzt* (Zl. 2), *ich, mich, wieder* (Zl. 3) im Vergleich zu allen übrigen *i*-Punkten. Es ist ferner auffallend die inconsequente Trennung des Buchstabens *c* von *h* in den Wörtern *mich* (Zl. 1), *ich, Euch* (Zl. 2) im Vergleich zu den übrigen *ch*. Die Isolierung des ersten Buchstabens eines Wortes kann ja auch begründet sein, aber hier ist sie auch nicht regelrecht durchgeführt. — Einzelne Unterbrechungen könnten freilich als natürlich und unwillkürlich angesehen werden, z. B. in den Wörtern *Wie* (Zl. 1), *hatte* (Zl. 2), *doch* (Zl. 2), *und* (Zl. 3), überhaupt jede Unterbrechung vor einem *o, a, c, e, d, g, i, u, t*, weil bei diesen Buchstaben der Aufstrich oft unwillkürlich d. h. aus Gewohnheit weggelassen wird. Ganz unnatürlich und gekünstelt sehen aber Unterbrechungen aus wie in den Wörtern: *elend* (Zl. 1), *verlassen, jetzt* (Zl. 2), *wieder, erholt, schicke* (Zl. 3) und ähnliche. Man kann also zusammenfassend sagen: wenn in einem Worte viele Bindungen vorkommen, und innerhalb dieses Wortes steht ein Buchstabe isoliert, dessen Schreibart zu einer Unterbrechung gar keinen Anlass gibt, z. B. *l* (vgl. *elend* Zl. 1), so darf ziemlich mit Sicherheit auf eine absichtliche Unterbrechung geschlossen werden. Im übrigen lohnt es sich immerhin, jedesmal die betreffenden gleichen Buchstaben an anderen Stellen des Schriftstückes bezüglich ihrer Gestaltung und beiderseitigen Verbindung mit dem verdächtig erscheinenden Buchstaben zu vergleichen und so die etwaige Notwendigkeit einer Unterbrechung zu erforschen. (Vgl. z. B. *s* im Worte *als* (Zl. 2) gegenüber dem *s* im Worte *verlassen* (Zl. 2) und *Los* (Zl. 4).

Digitized by Google

Sieht man nun die Wortendstriche des Originalschriftstückes etwas genauer an, so muss es sogleich auffallen, dass in einigen Wörtern die Wortendstriche horizontal verlaufen (d. h. nach rechts ausgezogen sind), z. B. in den Wörtern *Lieben, wie, fühlte* etc. (Zl. 1), während in anderen Wörtern der Wortendstrich in einer Rundung nach oben rechts ausgezogen ist, z. B. in den Wörtern *meine, elend* (Zl. 1), *ich, verlassen* (Zl. 2) etc. Ein dritte Art von Endstrichen ist nicht zu finden. Die horizontal nach rechts ausgezogenen Wortendstriche deuten nun die für die Buchstabengruppenbildung nötige Verbindung zweier Wörter an, während die nach oben rechts ausgezogenen Wortendstriche die natürliche Trennung zwischen den beiden Wörtern bestehen lassen. Solche absichtlich gewählte Wortendstriche bilden für den Graphologen ein weiteres unverkennbares Zeichen einer vorliegenden verdeckten Geheimschrift. Diese Wortendstriche veranlassen den Schreiber auch zu manchen Inconsequenzen, vgl. die Ansätze oben am Buchstaben *s* in den Wörtern *als* (Zl. 1), *schicke* (Zl. 2), *Los* (Zl. 4), sodann des Buchstabens *s* in den Wörtern *so* (Zl. 1), *verlassen* (Zl. 3).

Vom graphologischen Standpunkt aus muss man eingestehen, dass die Wortendstriche als Zeichen einer notwendigen Verbindung zweier Wörter zu jenem Zwecke nicht vorteilhaft gewählt sind, da man gerade diese am wenigsten für geeignet findet, eine absichtliche Veränderung an ihnen verbergen zu können. — Für viel zweckmässiger halte ich es aber, die Wortaufstriche als Kennzeichen einer notwendigen Verbindung zweier Wörter zu verwenden. Denn es ist absolut nicht aussergewöhnlich und auffällig, wenn ein Teil der Wörter mit einem Aufstrich beginnt, ein anderer Teil aber nicht, z. B. die mit *a, o, d, g, t, i, c, e, q, u* event. *v, w* beginnenden Wörter können, ohne jeglichen Verdacht zu erregen, den Aufstrich entbehren. Aber auch die übrigen Buchstaben wie *b, f, h, k, l* etc. können ihn teilweise entbehren, sodass der Aufstrich erst rechts vom Grundstrich des betreffenden Buchstabens beginnt. Ein fehlender bezw. verkürzter Wortaufstrich soll also hiernach beispielsweise die natürliche Trennung vom vorhergehenden Worte bestehen lassen. Bei solchen Buchstaben, die den Aufstrich aber nicht leicht entbehren können, z. B. *m, n, r, W* etc. kann man Trennungskennzeichen die nach innen gebogenen Aufstriche gelten lassen. —

Auf diese Weise wäre wohl ein auffallendes Moment bei dieser Geheimschrift ziemlich beseitigt. Wie steht es nun aber

Digitized by Google

mit den verdächtigen Unterbrechungen inmitten eines Wortes? Wie könnte man diese mit Vorteil umgehen?

Zur Lösung dieser Frage habe ich der verschiedenen Stellung der Uebersetzungszeichen und *t*-Querstriche eine besondere Bedeutung gegeben, indem ich hier je vier verschiedene Stellungen construierte und diesen jeweils eine andere Bedeutung beilegte: ich unterschied nämlich niedrig- und hochgesetzte, nach links und nach rechts*) gesetzte Uebersetzungszeichen und *t*-Querstriche. So kann also beispielsweise ein niedrig, nach links gesetzter *i*-Punkt bedeuten, dass direkt links von diesem *i* die notwendige Unterbrechung hätte vorgenommen werden müssen, ein hoch, nach links gesetzter *i*-Punkt, dass vor dem ersten Buchstaben links (von dem betreffenden *i*) die Unterbrechung zu suchen sei; eine analoge Bedeutung gab ich dem nach rechts niedrig und hoch gesetzten *i*-Punkt. Auf gleiche Weise sind die Uebersetzungszeichen von *ä, ö, ü, u,* die Ueberstriche bei *m* und *n* ($\bar{m}$, $\bar{n}$ zum Zeichen einer Verdoppelung) und der Querstrich von *t* zu behandeln. Soll aber durch ein Uebersetzungszeichen oder einen Querstrich keine Unterbrechung angedeutet werden, dann werden dieselben genau nach der Schulvorlage gesetzt. Wenn nun diese Hilfsmittel nicht ausreichend wären, um eine notwendige Unterbrechung anzuzeigen, so wendet man eben eine thatsächliche Unterbrechung an oder, falls dies zu auffallend wäre, deutet man die Unterbrechung durch einen unscheinbaren Punkt oder Strich, oder durch irgend eine andere graphische Eigenheit an der betreffenden Stelle an, z. B. durch verkürzte Schlussaufstriche bei Buchstaben wie *g, h, j,* oder durch offene und geschlossene *o, a, g, d,* oder durch besonders verabredeten Gebrauch von Haar- und Grundstrich, von runden und eckigen Formen des Buchstabens, ferner durch sinistrogyre und dextrogyre**) Schreibformen beim *u*-Häkchen, beim *d* und bei allen möglichen Endstrichen; sodann durch Einschalten von deutschen bezw. lateinischen Buchstaben oder Drucktypen an Stelle des regelrechten Buchstabens, weiter durch nach unten verlängerte Schlussabstriche beim *h, k, m, n, p, A, B, C, E, R* etc., durch enge, weite oder ausgefüllte Schleifen bei Buchstaben wie *l, k, h, g* etc., durch lange Wortanfangs- und Wortendstriche, durch verabredete Höhen- und Tiefendauer der Schriftzeichen, ferner durch

*) d. i. links und rechts von dem betreffenden Buchstaben aus, zu dem die Uebersetzungszeichen gehören.

**) d. i. links- und rechtsstrebende Schreibbewegung.

Digitized by Google

Schriftweite, durch enge und weite Zwischenräume zwischen den einzelnen Wörtern, durch die Lage der Schriftzeichen, auch durch Unterstreichungen, durch Interpunktionen, durch Weglassungen und Hinzufügungen von minderwertigen Buchstabenteilen — kurzum durch alle nur denkbaren Schriftveränderungen, die lediglich für das Auge des Graphologen wahrnehmbar sind.

Alle diese graphischen Möglichkeiten bieten eine mannigfaltige Abwechslung in der Kennzeichnung einer in obiger Geheimschrift nötigen Unterbrechung zum Zwecke der Bildung von Buchstabengruppen; ebenso lassen sich jene graphischen Möglichkeiten als Zeichen einer Verbindung oder Trennung zweier Wörter verwenden, sodass jene ursprünglichen einseitigen und für das Auge des Graphologen auffallenden Unterscheidungsmerkmale wesentlich verbessert werden können und so zur grösseren Sicherheit des Geheimnisses beitragen.

b) Die Graphologie zur Bildung neuer Geheimschriften.

V.

Graphologische Geheimschriftmethoden.

1. Die im vorstehenden Capitel aufgezählten graphischen Eigenheiten lassen sich nun auch direkt als Punktierzeichen nach Analogie der oben besprochenen Punktiermethoden verwerten. Wie bei dieser Art von Methoden durch kleine unscheinbare Punkte, Striche oder Nadelstiche der Chiffrebuchstabe geheim erkenntlich gemacht wird, so geschieht dies in der „graphologischen Punktiermethode“ durch eine der zahlreichen graphischen Eigenheiten.

Wie in einem Stenographiesystem die Hoch- und Tiefsetzung, die nahe und weite Entfernung eines Buchstabens, Haar- und Grundstrich eines Zeichens ihre besondere Bedeutung haben, ähnlich ist dies auch hier der Fall (vgl. z. B. die verschiedene Setzung der Uebersetzungszeichen und des t-Querstrichs, ferner die Enge und Weite einer Schleife etc.) Darum glaube ich, dass diese Methode am besten

„stenographologische Punktiermethode“

zu nennen sei.

Digitized by Google

Nachstehend soll ein Beispiel eines solchen stenographologischen Punktieralphabetes folgen:

a lässt sich z. B. kennzeichnen durch veränderte Lage des 2. Abstriches;*)

b „ „ „ „ „ „ weite Schleife;

c „ „ „ „ „ „ Fehlen des Aufstriches;

d „ „ „ „ „ „ Schleifenbildung beim 2. Abstrich;

e „ „ „ „ „ „ ausgefüllte Schleife;

f „ „ „ „ „ „ Fehlen des Schlussaufstriches;

g „ „ „ „ „ „ enge Schleife unterhalb der Zeile;

h „ „ „ „ „ „ dextrogyre Bogenbindung nach dem 1. Abstrich;

i „ „ „ „ „ „ links gesetzten J-Punkt;

k „ „ „ „ „ „ sinistrogyre Bogenbindung (d. i. Schleifenbildung) nach dem 1. Abstrich;

l „ „ „ „ „ „ steile Stellung;

m „ „ „ „ „ „ verkürzte Höhendauer des 2. und 3. Ab- bezw. Aufstriches;

n „ „ „ „ „ „ Winkelbindung nach dem 2. Aufstrich;

o „ „ „ „ „ „ Offenlassen dieses Buchstabens;

p „ „ „ „ „ „ sinistrogyre Schleifenbindung (sog. Knoten) beim 2. Abstrich;

q̇ „ „ „ „ „ „ spitz auslaufenden (2.) Abstrich;

r „ „ „ „ „ „ Schleifenbildung nach dem 2. Aufstrich;

s „ „ „ „ „ „ Abschliessen des Abstriches mit einem Punkt;

t „ „ „ „ „ „ rechts angesetzten t-Querstrich;

u „ „ „ „ „ „ niedrig gesetzten u-Haken;

*) Bei diesen Beispielen ist die lateinische Schreibweise als Grundlage benutzt.

Digitized by Google

v lässt sich z. B. kennzeichnen durch Höhersetzen der Schleife (oben rechts);
w „ „ „ „ „ „ hochgesetzte Schleife (rechts oben);
x „ „ „ „ „ „ Ausfüllen der ersten Schleife;
z „ „ „ „ „ „ Fehlen jed. Druckstriches;

Gleiche oder ähnliche graphische Eigenheiten können auch bei Kennzeichnung grosser Buchstaben (Majuskeln) verwendet werden.

Ebenso bei Ziffern; es lässt sich z. B.

1 kennzeichnen durch überwiegenden Druck beim Abstrich;
2 „ „ Schleifenbildung an der Basis (unten links);
3 „ „ einwärts gebogenen Aufstrich;
4 „ „ Ausfüllen der Schleife nach dem 1. Abstrich;
5 „ „ sinistrogyr verlaufendes Häkchen (oben);
6 „ „ spitz auslaufenden Schlussabstrich;
7 „ „ dextrogyr auslaufenden Schlussabstrich;
8 „ „ grössere Schleifenbildung an der unteren Hälfte;
9 „ „ Fehlen der Druckstellen;
0 „ „ enge Schleife.*)

Eine derartige Kennzeichnung von Schriftzeichen (d. i. Punktierung) hat natürlich lediglich den Zweck, die als Chiffrebuchstaben bezeichneten Schriftzeichen von anderen gleichen Schriftzeichen unterscheidbar zu machen, sodass ein Concept der geheimen Mitteilung zu empfehlen ist.**)

Selbstverständlich wird man bei Anwendung einer graphologischen Geheimschriftmethode im Interesse der Sicherheit des Geheimnisses die geheime Mitteilung zuerst nach einer bekannten Methode (des ersten Abschnittes d. W.) chiffrieren, sodass mit der Entdeckung der graphischen Abnormitäten nicht zugleich das Geheimnis selbst klarliegt. — Die Sicherheit des graphologischen Geheimnisses hängt nun ganz allein von der geschickten Einführung und Anwendung der graphischen Chiffriernüancen ab: je weniger

*) Zum leichteren Verständnis der obigen und zur Anwendung anderer Schrifteigenheiten empfehle ich das bereits citierte Lehrbuch Busse's. (Die Handschriften-Deutungskunde. „Graphologie-Unterricht in Briefen.")

**) Hierher gehören auch die Verbesserungen der beiden Geheimschriften Cap. III. und IV. dieses Abschnittes, soweit dabei graphologische Principien zu Grunde gelegt wurden.

Digitized by Google

diese also von den normalen Schrifteigenheiten des Schreibers abweichen, desto unauffälliger werden jene graphischen Abnormitäten dem nichteingeweihten Graphologen erscheinen, von einem Laien gar nicht zu reden. — Es wird auch einleuchten, dass das Mass der Sicherheit des graphologischen Punktier-Geheimnisses von der Kenntnis graphologischer Grundsätze des Schreibers abhängt.

---

2. Den Schrifteigenheiten leichter anzupassen ist die nachstehende graphologische Geheimschriftmethode. — Ihr Grundgedanke ist der, dass durch schärferes Ausprägen einer regelmässig wiederkehrenden Schrifteigenheit dem Correspondenten erkennbar gemacht wird, in welchem Worte er einen Chiffrebuchstaben zu suchen hat. Der Chiffrebuchstabe selbst soll dann angedeutet werden durch die verschiedene Setzung der Uebersetzungszeichen und des t-Querstriches (vgl. Cap. IV. dieses Abschnittes), oder einfacher durch die Verabredung, dass der 2., 3., 4 etc. Buchstabe des graphisch bezeichneten Wortes als Chiffrebuchstaben zu gelten habe. —

Um das Wort, (das den Chiffrebuchstaben enthält), selbst zu kennzeichnen, hat der Schreiber irgend eine vorherrschende Eigenheit seiner Handschrift ausfindig zu machen, an welcher er leicht eine Veränderung vornehmen kann, ohne den Schein der Willkür zu erwecken; am besten eignet sich dazu nach meiner Ansicht des Wortes Anfang oder Schluss. Ich will hier einige Beispiele gut anwendbarer graphischer Eigenheiten folgen lassen:

Lange gerade Aufstriche am Beginn des Wortes, die bekanntlich den Widerspruchsgeist bekunden, sind insofern gut als graphische Punktierzeichen zu gebrauchen, weil ohne besondere Berechnung eine nur dem eingeweihten Correspondenten erkennbare Veränderung an jener Eigenheit vorgenommen werden kann, indem man — den übrigen ähnlichen Zeichen d. i. Eigenheiten gegenüber — den betreffenden Aufstrich länger oder kürzer macht, oder ihn unter einem spitzeren oder stumpferen Winkel zur Schreiblinie legt, oder indem man ihn — falls es nicht dem allgemeinen Schriftductus widerspricht — mit einem sog. Eigensinnshäkchen versieht, dessen Gestalt und Lage übrigens auch selbständig als graphisches Punktierzeichen dienen kann. Wenn nämlich einer Handschrift die Zeichen des Widerspruchsgeistes fehlen, aber die Zeichen der Hartnäckigkeit und des Eigensinns vertreten sind, so

Digitized by Google

lassen sich diese Zeichen auch als graphische Punktierzeichen verwenden, sowohl am Wortanfang als am Wortschluss.

Verlaufen die langen Wortaufstriche im Bogen, so kann man hier vor allem die Anwendung von Druckstellen entscheiden lassen.

Mangelt es einer Handschrift an Aufstrichen, besonders an langen, so mag das Fehlen oder Vorhandensein eines Aufstriches das betreffende Wort andeuten.

Am Schlusse eines Wortes können als graphische Punktierzeichen besonders dextrogyre und sinistrogyre Endstriche massgebend sein, auch Kürze, Länge und Fehlen des Endstriches. Selbst das Mass der Zwischenräume (zwischen den einzelnen Wörtern) sowie die auf- oder absteigende Richtung eines einzelnen Wortes (nicht der Zeile) können zur Kennzeichnung des betreffenden Wortes behilflich sein. —

Mag eine abänderungsfähige Schrifteigenheit gewählt werden, welche sie immer sei, sie muss stets mit entsprechenden Eigenheiten der Handschrift in Einklang stehen oder gebracht werden können, wenn sie nicht dem Uneingeweihten auffallend und unwillkürlich erscheinen soll.

Daher werden im Prinzip auch nur solche Schrifteigenheiten jeweils in Betracht kommen, die thatsächlich dem Schriftductus des Schreibers angehören; denn es ist nicht so leicht, irgend eine für die Kennzeichnung bequeme Schrifteigenheit einzuführen und consequent durchzuführen! Deshalb wird man sich beim Mangel einer verwendbaren Haupteigenheit der Schrift darauf beschränken müssen, unter Zugrundelegung verschiedener Nebeneigenheiten die Bezeichnung (Punktierung) der einzelnen Wörter vorzunehmen. —

(Schrifteigenheits-Punktiermethode.)*)

Bei Anwendung einer graphologischen Geheimschriftmethode darf man nicht den Umstand aus dem Auge lassen, dass solche Methoden nur geeignet sind, Geheimnisse in der Handschrift d. h. die Existenz einer geheimen Mitteilung zu verbergen, während die Chiffreschrift selbst mit Hilfe einer der zahlreichen Versetzungsmethoden (s. I. Abschnitt) erst hergestellt werden muss, indem nämlich die einzelnen Buchstaben der Klarschrift zunächst versetzt und dann die Chiffrebuchstaben durch eine graphologische Methode in der Handschrift, d. i. in einem Schriftstück gleich

*) Vgl. „Graphologische Monatshefte“ 1899, No. 8/9, S. 123. —

Digitized by Google

giltigen Inhalts, dem Correspondenten erkenntlich gemacht werden. Zu erfolgreicher Anwendung einer Geheimschrift ist immer eine Combination mindestens zweier Geheimschriftmethoden zu empfehlen. Auf diese Weise bleibt, wenn auch die Existenz einer Geheimschrift entdeckt wird, unter Umständen doch das Geheimnis der Mitteilung selbst gewahrt. Der gefangene Verbrecher aber wird seine ganze Hoffnung auf die Sicherheit der graphologischen Geheimschriftmethode stützen und mit ihrer Entdeckung sein Hauptgeheimnis preisgegeben sehen. —

Meine Ausführungen in diesem Abschnitte werden erkennen lassen, dass die Graphologie für die Geheimschriftenkunde einen doppelten Wert hat. Auf der einen Seite leistet sie uns eine nicht zu unterschätzende Hilfe bei der Entdeckung einer in dem Schriftstück selbst verborgenen Geheimschrift, auf der anderen Seite ermöglicht sie uns mancherlei wertvolle Verbesserungen und Variationen bekannter Methoden. —

Es ist allerdings nur dem geübten Graphologen möglich, die feinen geheimen Nüancierungen an Schriftzeichen derart vorzunehmen, dass sie selbst für das Auge des prüfenden Graphologen unkenntlich sind. Eine erfolgreiche Anwendung graphologischer Geheimschriftmethoden bedingt also graphologische Kenntnisse.

Digitized by Google

Anhang.

Drei neue Geheimschriftmethoden.

Während ich im vorigen Abschnitte den Wert der Graphologie für die Entzifferung, Verbesserung und Neubildung von Geheimschriften darzulegen bestrebt war, will ich hier noch einige neue (noch nicht veröffentlichte) Methoden besprechen, die allerdings nicht auf graphologischen Grundsätzen beruhen, die vielmehr die Anwendung solcher Grundsätze in dem Sinne vermeiden, dass sich die Existenz der geheimen Mitteilung am allerwenigsten auf Grund graphologischer Untersuchungen entdecken lässt. Wenn zur Entdeckung der Existenz der geheimen Mitteilung (besonders bei der Methode 2 und 3) nicht der Zufall mitspielt, so wird eine Entdeckung mit Recht zu bezweifeln sein.

1. Der Orthographiechiffre.

Wie bei den graphologischen Methoden am einzelnen Buchstaben Veränderungen vorgenommen werden, so geschehen beim Orthographiechriffre die Veränderungen am Worte selbst. Hier kommen in Betracht scheinbar nachlässige Weglassungen von Buchstaben, die nach dem Sinne des Wortes leicht zu ergänzen sind, z. B. *jetz* statt jetzt, *nich* statt nicht, *pötzlich* statt plötzlich etc., ferner Orthographiefehler z. B. *dankent* statt dankend, *Zeicher* statt Zeiger, *Apell* statt Appell etc., ferner scheinbar nachlässig falsch gesetzte Buchstaben, die uncorrigiert stehen bleiben, aber doch nicht den Sinn des Wortes stören, z. B. in *aller* Beziehungen statt in allen Beziehungen (Flexionsfehler), oder gegen *mir* statt gegen mich (Dialektfehler); endlich Hinzufügungen von überflüssigen Buchstaben z. B. *Theil* statt Teil, *Schifffahrt* statt Schiffahrt, *Eeiche* statt Eiche etc. Alle diese Wortfehler ermöglichen es,

Digitized by Google

dem fortgelassenen bezw. überflüssig oder falsch gesetzten Buchstaben eine geheime Bedeutung beizulegen. Ebenso können auch Silben oder ganze Wörter solche Mängel an sich tragen: auch sie können fortgelassen werden, überflüssig oder falsch gesetzt sein, ohne den Sinn des Satzes zu stören. Fortgelassen können z. B. werden: ich, wir, ebenso Artikel etc.; hierher gehören auch alle Abkürzungen eines Wortes. Ueberflüssig gesetzt können werden z. B. eine scheinbar nachlässige Wiederholung derselben Silbe, desselben Wortes; auch die meisten Partikeln (z. B. nun, also, wohl, ja, denn etc.) können als solche überflüssige Silben im Satze behandelt werden. Es können auch Silben und Wörter geschrieben werden, die dem Sinne nach nicht in den Zusammenhang des Satzes gehören, diesen aber nicht beeinträchtigen; sie können eingeklammert oder so durchstrichen werden, dass man sie noch lesen kann. Auch diese Art von Zusätzen kann mit geheimen Bedeutungen verknüpft werden.

2. Der Referatchiffre.

Die durchaus originelle Geheimschrift eines Nihilisten (Meth. IV., III. Abschnitt; bezw. Methode XVIII, I. Abschnitt) entdeckt, wie ich oben erwähnte, dem Graphologen manche Mängel, die aber zum Teil mit Hilfe graphologischer Momente beseitigt werden können. Nicht allzuferne lag hier die Frage, ob nicht eine Geheimschrift derart in einem ostensiblen Schriftstück zu verbergen sei, dass selbst mit graphologischen Hilfsmitteln nichts auszurichten sei. Eine Lösung dieser Frage ist z. B. folgende:

Der mitteilende Correspondent schreibt einen Bericht (Referat) nieder über irgend ein Ereignis (beispielsweise über einen Unglücksfall, über eine Bergpartie etc.), der ihm Gelegenheit bietet, in ganz natürlichem und ungezwungenem Stile mehrere Zahlen anzuwenden. Die in den Zusammenhang des Berichtes eingeflochtenen Zahlen sollen dann auf gewisse Buchstaben des Berichtes hinweisen, die, zusammengestellt, die geheime Mitteilung ergeben. Ein Beispiel wird dies klar machen:

„ . . . . Als wir in W. angekommen waren, rasteten wir ein wenig und gingen dann wieder zu Fuss weiter — dem Gebirge zu. Bald standen wir vor einem Berg, der etwa 18 Hundert Meter hoch war. Unsere Truppe war 6 Mann stark. Anfangs ging es gut vorwärts; als wir in der Höhe von etwa 9 Hundert

Digitized by Google

Metern waren, machten wir Halt. Es war gerade 10 Uhr 25 Minuten des Morgens, als wir dort angelangt waren. Nach einer Ruhepause von 30—40 Minuten setzten wir unsern Marsch weiter; nach einiger Zeit stiessen wir auf eine in das Gestein eingehauene Treppe mit 44 oder 45 Stufen (wie ich zählte). Da dieselbe sehr mangelhaft war, rutschte ich mindestens 3 Mal aus, wurde aber jedesmal durch meinen Hintermann vor einem Absturz bewahrt . . . .".

Wer diesen harmlosen Bericht liesst, wird nicht sagen können, dass er Verdacht erregen könnte; (allerdings dann schon, wenn aus den Verhältnissen des Schreibers zu ersehen wäre, dass er nicht Teilnehmer oder Zeuge des berichteten Geschehnisses sein konnte, z. B. ein Gefangener).

Die in dem Berichte vorkommenden Zahlen verweisen den Empfänger des Schriftstückes auf die entsprechenden Buchstaben — vom Anfang des Berichtes aus gezählt; also:

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19
a l s w i r i n W a n g e k o m m e n
20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38
w a r e n r a s t e t e n w i r e i n
39 40 41 42 43 44 45 46
w e n i g u n d . . . . .

Somit bedeuten die in dem Berichte vorkommenden Zahlen:

18 6 9 10 25 30 40 44 45 3
e r w a r t e u n s. —

Natürlich lässt diese Methode eine Reihe Variationen zu. (Vgl. Cap. III, Schluss, III. Abschnitt; ferner den Schlussabsatz von Cap. V, desselben Abschnittes).

Zu diesem Referatchiffre eignen sich am besten Rechnungs- und statistische Berichte, in welchen mehr Zahlen unmittelbar aufeinanderfolgen können, ohne Verdacht zu erregen. — Hierbei ist man nicht, wie z. B. bei der Methode II., III. Abschnitt (Netzchiffre) oder bei Heidels Punktiermethode (Methode XXVII, I. Abschnitt) an gewisse Grenzen gebunden, sondern kann die Zahl — allerdings in geordneter Reihenfolge — im Laufe des Berichtes einschalten, wann sich gerade Gelegenheit bietet, sodass damit unnatürliche und gezwungene Redensarten von vornherein ausgeschlossen sind, was aber bei jenen beiden Methoden nicht der Fall ist. —

Digitized by Google

3. Die Reduktionsmethode.

Es gilt hier, die Frage zu lösen, ob eine geheime Mitteilung derart in einer ostensiblen Nachricht zu verbergen sei, dass sowohl ihre Existenz unkenntlich bleibt, als auch durch Einwirken einer dritten Person unwillkürlich nicht zerstört werden könne. Diese Frage wird nämlich actuell bei telegraphischer Uebermittelung eines Geheimnisses. Lässt sich nun eine Methode ausfindig machen, mit deren Hilfe eine geheime Mitteilung in einer harmlosen Depesche so zu verbergen ist, dass der Telegraphenbeamte weder aus irgend welchen Merkmalen z. B. der ungewöhnlichen Länge der Depesche, (abgesehen von den chiffrierten Depeschen die aber nunmehr für den Privatverkehr ausgeschlossen sind; siehe oben den Schluss der allgemeinen Anwendungsregeln,) Verdacht schöpfen, noch durch die Operation mit dem Telegraphen dem Empfänger der geheimen Depesche die Kennzeichen derselben vernichten kann? Mit graphologischen Principien lässt sich hier natürlich nichts anfangen. Es war vielmehr die Geheimschrift des Nihilisten (Methode XVIII. Abschnitt I.), die ich der Lösung dieser Frage zu Grunde legte. Bei der oben (Cap. IV. Abschnitt III.) beschriebenen Verbesserung dieser Geheimschriftmethode waren nur graphische Eigenheiten massgebend, die aber durch Einwirkung dritter Personen unwillkürlich vernichtet würden (z. B. durch blosses Abschreiben). Es musste nun irgend eine Variation gefunden werden, durch welche eine dem Empfänger angedeutete Buchstabengruppe unter keinen Umständen verändert werden könnte, ohne dass dadurch ein Wort bezw. der Inhalt der Depesche selbst verändert würde. Dies ist sogar sehr einfach, wenn man die Anzahl der Gruppenbuchstaben zusammenfallen lässt mit der Anzahl der Wortbuchstaben, mit andern Worten: das Ende eines jeden Wortes muss auch zugleich das Ende einer Buchstabengruppe sein. Allerdings scheint eine Schwierigkeit zu bestehen, wenn die Gruppe — was sehr oft vorkommt — nur einen Buchstaben enthalten soll, während die deutsche Sprache nur ein einziges Monogramm (d. i. einsilbiges Wort mit 1 Buchstaben) hat, nämlich das Ausrufewörtchen: *o!* Diesen Mangel beseitigt man aber leicht dadurch, dass man mit seinem Correspondenten vereinbart, dass alle Wörter, die man gewöhnlich abkürzt, z. B. und (u.), und so weiter (u. s. w.), und dergleichen (u. dgl.), unter anderen (u. a.) etc., sodann alle Artikel, gewisse Partikeln, ferner Ziffern und Zahlen (nach der vorhergehenden Methode in den Inhalt der Mitteilung aufgenommen)

Digitized by Google

und andere oft vorkommende Wörter als eine Buchstabengruppe von nur 1 Buchstaben zu gelten haben; es wird hier also die Anzahl der Buchstaben eines Wortes auf 1 reduziert (Reduktion).

Ausserdem kann man auch so verfahren, dass die Buchstabenanzahl aller Wörter um 1 vermindert wird (d. h. also, dass die Glieder eines Wortes jeweils auf x—1 reduziert werden), sodass z. B. Trigramme als Bigramme, und Bigramme (wie z. B. in, an, zu, wo, da etc.) als Monogramme zu gelten haben, wodurch der thatsächliche Mangel an Buchstabengruppen von 1 Glied (d. i. Monogrammen) beseitigt wird. —

Die Chiffrierung und Dechiffrierung nach der soeben besprochenen Methode geschieht analog wie bei der oben citierten Methode XVIII im I. Abschnitt.

Digitized by Google

Schlusswort.

Alle die hier beschriebenen Geheimschriftmethoden lassen sich in erster Linie und auch am besten im schriftlichen Privatverkehr anwenden. Für den telegraphischen Verkehr muss man sich — wie oben bei den allgemeinen Regeln erwähnt — besonders vorgeschriebener Wörter bedienen, die in eigenen Telegraphiewörterbüchern zusammengestellt sind. Allein es gibt auch Mittel und Wege, diese Vorschriften zu umgehen, wenn man sich einer im Anhang besprochenen Methode bedienen wollte, was aber nur bei ganz kurzen streng-geheimen Mitteilungen zu empfehlen wäre.

Beim Militär und ganz besonders in Kriegsfällen tritt die geheime Verständigungsweise in den Vordergrund. Im schriftlichen Verkehr, der entweder durch Telegraphie oder besondere Boten vermittelt wird, bedient man sich vornehmlich der sog. „Patronenchiffres". Da es nun aber ausserordentlich viele Fälle gibt, in denen man durch feindliche Stellungen gehindert ist, chiffrierte Depeschen auszutauschen, hat man auch wieder Auswege gefunden, diese ernsten Hindernisse zu überwinden. So kam im letzten südafrikanischen Kriege sehr häufig der sog. „Heliograph" in Anwendung, dessen Hauptbestandteil ein drehbarer Spiegel ist, durch den verabredeterweise Sonnenstrahlen in die Ferne projiciert werden, sodass sich z. B. die Belagerten mit den heranrückenden Ersatzcorps verständigen können. Da aber die Sonne oft gerade im gelegenen Augenblick als Vermittlerin versagt, namentlich bei Anbruch der Nacht, so musste auch da Abhilfe geschaffen werden. Und so werden in allerneuester Zeit electrische Glühlämpchen mit verschiedenfarbigem Glas derart eingerichtet, dass sie auf die Lanzen der Cavallerie aufgeschraubt werden können, sodass man sich durch verabredete Manipulationen mit fernstehenden Kriegskameraden verständigen und so eine einstweilige Fühlnng herstellen kann; diese Einrichtung soll auch im europäisch-chinesischen Krieg in Anwendung gelangt sein. —

Digitized by Google

Geheime Verständigungsweisen dieser Art gehören aber nicht mehr in den Rahmen obiger Darstellung, weswegen eine blosse Erwähnung hier genügen mag, was auch der Fall sein dürfte mit einigen anderen öfters angewandten geheimen Verständigungsweisen durch allegorische Zeichen und Geberden, ich meine vor allem die „Blumen- und Briefmarkensprache", sowie die „Hand- oder Fingersprache", wie sie bei internationalen Gaunern in Uebung ist; über die letzte Verständigungsart gibt Prof. Dr. Hans Gross in seinem lehrreichen „Handbuch für Untersuchungsrichter" (3. Aufl. 1898) genügenden Aufschluss. —

Digitized by Google

Ein fachmännisches Urteil über das Werk.

„. . . . . Ihre sehr gründliche und instructiv geschriebene, sowie sehr übersichtlich systematisierte Arbeit hat mich in hohem Grade interessiert, und zwar besonders wegen der durchaus neuen und wichtigen Berücksichtigung der Graphologie; hierdurch haben Sie nicht nur die Geheimschriftkunde, sondern auch die Graphologie in ihrer praktischen Verwendung wesentlich gefördert. Ich zweifle demnach nicht, dass Ihr Werk in allen Kreisen, die sich mit Geheimschrift oder Graphologie beschäftigen, das gleiche Interesse finden wird, wie bei mir. Ich werde gerne bereit sein, Ihre „Moderne Geheimschriften" an geeigneten Stellen zu empfehlen. . . . . —"

Hans H. Busse

Institut für wissenschaftliche Graphologie

München.

Digitized by Google

Graphologische Monats-Hefte.

Organ der Deutschen graphologischen Gesellschaft.

Verlag von Karl Schüler (A. Ackermann's Nachflg.), kgl. bayr. Hofbuchhandlung, München.

Einzige deutsche Zeitschrift für wissenschaftliche Handschriften-Deutungskunde. 1897 gegründet. Reich illustriert.

Für Mitglieder der „Deutschen graphologischen Gesellschaft" gratis und franko.

Für Nichtmitglieder im Abonnement: 8 Mk.;

Preis des einzelnen Heftes 80 Pfg.

Postzeitungspreisliste No. 357a.

Die Publicationen der „Deutschen graphologischen Gesellschaft" sind die bedeutendsten Erscheinungen der deutschen graphologischen Litteratur während der letzten Jahre. Zu den Mitarbeitern gehörten u. a.: Hans H. Busse, H. W. Cornelis, J. Crépieux-Jamin, Iwan Döry, Dr. Ludwig Klages, Johannes Marer, Dr. med. F. Maack, Dr. med. Georg Meyer, Dolph. Poppée, Prof. Dr. W. Preyer, Hans Schneickert, Isabelle Baronin Ungern-Sternberg.

I. Jahrgang; 1897. „Berichte". I.

172 Seiten. Mit über 50 Facsimiles und mit einem Portrait Prof. W. Preyer's.

elegant gebunden 10 Mk.

Nur noch wenige Exemplare.

II. Jahrgang; 1898. „Berichte". II.

180 Seiten. Mit über 70 Facsimiles im Text, mit 6 Handschriften-Beilagen und einem Portrait des Abbé J.-H. Michon.

ungebunden 6 Mk., elegant gebunden 8 Mk.

III. Jahrgang; 1899. „Graphologische Monatshefte". I.

180 Seiten. Mit Vignetten von E. Weigel, mit über 120 Schriftproben und Figuren im Text und mit einem Portrait J. Crépieux-Jamin's.

ungebunden 5 Mk., elegant gebunden 7 Mk.

IV. Jahrgang; 1900. „Graphologische Monatshefte". II.

160 Seiten. Mit über 100 Schriftproben und Figuren im Text und mit einem Portrait Hans H. Busse's.

ungebunden 5 Mk., elegant gebunden 7 Mk.

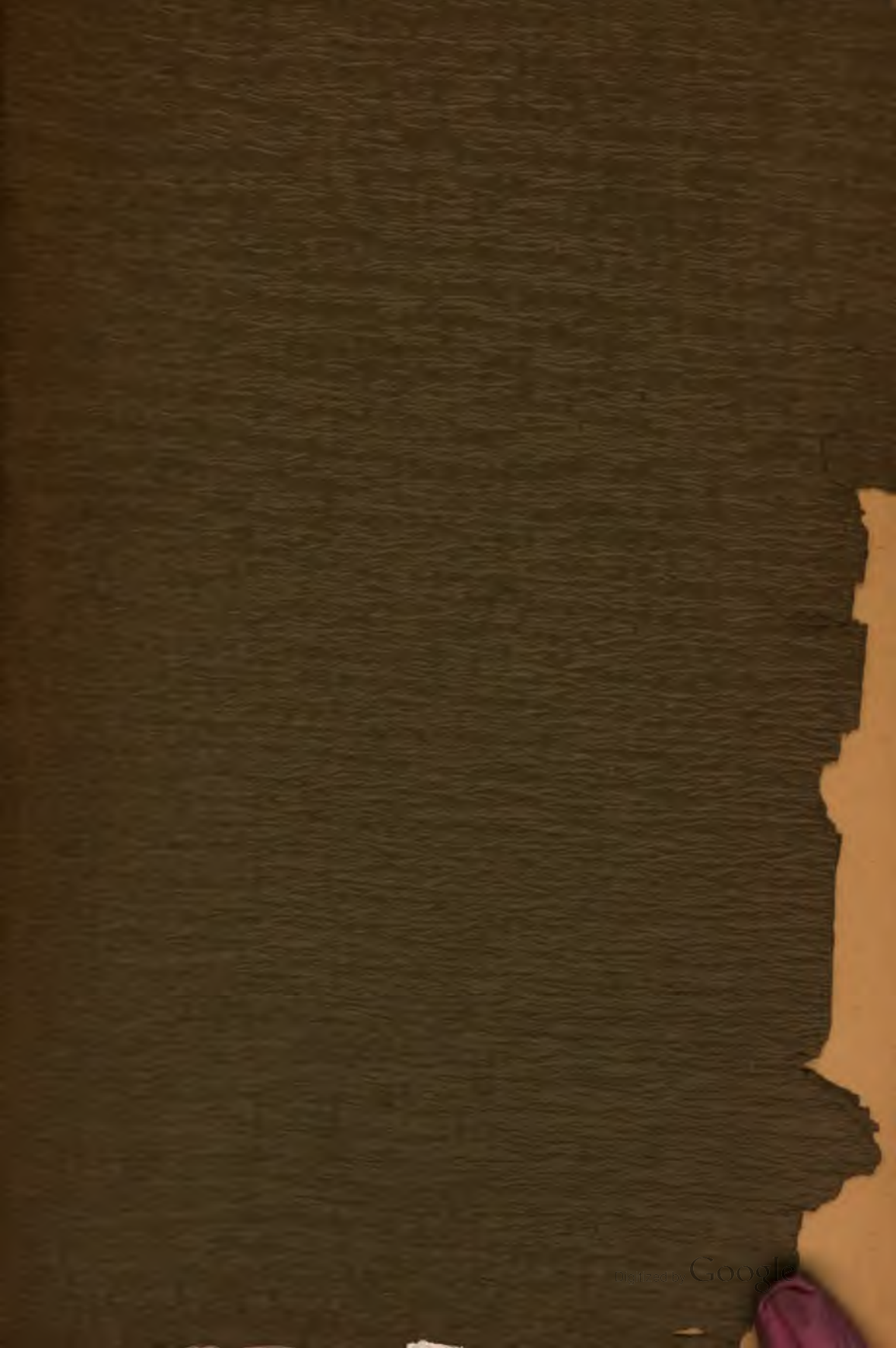
Alle vier Jahrgänge zusammen: gebunden 30 Mk.

Abonnements nimmt jede Zeitungs-Expedition der Post und jede Buchhandlung entgegen.

Probe-Nummern gratis und franko.

Bestellungen sind zu richten an die Expedition der „Graphologischen Monats-Hefte" in München.

Digitized by Google


Digitized by Google

Digitized by Google

Digitized by Google

Digitized by Google